La protection des données (à caractère personnel) à l'heure de l'Internet

HENROTTE, Jean-François; Poullet, Yves

Published in:
Protection du consommateur, pratiques commerciales et T.I.C.

Publication date:
2009

Document Version
le PDF de l'éditeur

5

La protection des données (à caractère personnel) à l'heure de l'Internet[1 2]

Yves POULLET
professeur à l'U.Lg. et aux F.U.N.D.P.
directeur du CRID – F.U.N.D.P.
Président du comité de rédaction de la R.D.T.I.
avec la collaboration de

Jean François HENROTTE
avocat
directeur de la R.D.T.I.

SOMMAIRE

Cet article s'inscrit dans le cadre des recherches entreprises par le CRID dans le cadre du projet MIAUCE, projet du 6e programme-cadre de l'Union européenne analysant certaines technologies multimodales de surveillance (*Multi modal Analysis and Exploration of Users within a controlled Environment*, IST Call 5, FP6-2005-IST-5). Les auteurs remercient les chercheurs du CRID travaillant sur ce projet pour leur apport, en particulier Antoinette ROUVROY, docteur en droit et chercheur qualifiée F.N.R.S. et Denis DARQUENNES, informaticien et physicien.

2. Pour un exposé introductif sur la législation relative à la protection des données à caractère personnel, voir S. LOUVEAUX et C. de TERWANGNE, « Protection des données à caractère personnel : application en Belgique de la directive européenne » *in Actualités du droit des techniques de l'information et de la communication*, Liège, CUP, 2001, vol. 45, pp. 9-34.

1. La société de l'information : des interrogations

Les données nous concernant circulent partout sur la toile de nos réseaux de communication moderne. Plus d'un milliard de personnes furètent sur l'Internet. Les mobilophones se multiplient et demain la technologie permettra de combiner les avantages du téléphone portable, de l'ordinateur et de l'appareil de télévision. Le nombre de fichiers dans lesquels figure en moyenne un européen célibataire se monte à plus ou moins 500 [3]. Le rappel de ces chiffres et de cette convergence induisent quelques questions :

Quelles données circulent à notre propos ? Nous en devinons certaines mais en ignorons bien d'autres ! Les modes de collecte de ces données se multiplient, caméras de vidéosurveillance, *Radio Frequency Identifiers* (RFID) [4] lisibles à distance, parfois à partir de capteurs situés dans les mobilophones [5] ; les données collectées croissent de même, allant des données que je place sur *Facebook*, les données de trafic et de localisation, mon empreinte digitale, l'A.D.N. de mon chien, mes recherches sur mon engin de recherche favori, la direction de mes yeux [6].

Qui traitent ces données ? Sans doute les noms de notre banquier, de notre assureur, de notre employeur, de telle ou telle administration, nous apparaissent évidents, mais combien d'autres nous épient ? Le nom de DoubleClick, société de *cybermarketing* opérant grâce à des *cookies* envoyés lors de la visite de sites associés à cette société, peut être cité.

C'est cette société rachetée récemment par *Google*, qui, à partir des données collectées grâce aux *cookies* introduits dans le disque dur de l'utilisateur

Yahoo aurait collecté, en 2007, 110 milliards de données sur ses sites aux États-Unis, soit une moyenne de 811 informations par internaute, selon une étude ComScore (http://www.neteco.com/129652-donnees-personnelles-societes-net-consommatrices.html?xtor=EPR-1).

ou autres puces sans contact (*Near Field Communication* (N.F.C.)).

Il est possible d'utiliser de manière complémentaire ces modes de collecte : ainsi, la possibilité à partir de capteurs placés dans des mobilophones de repérer la présence d'une personne à proximité d'un objet sur lequel est placé un tag, c'est-à-dire une puce lisible à distance. Sur les expériences menées aux États-Unis et le débat suscité par l'utilisation combinée des technologies des RFID et de la mobilophonie, lire N. KING, « Direct Marketing, Mobile Phones and Consumer Privacy Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices », *Federal Communications Law Journal*, March 2008, 2, Vol. 60, pp. 229 et s.

Dans le cadre des projets analysés par le projet MIAUCE, un projet concerne l'analyse automatique du regard et des expressions de la physionomie du visage pour en déduire les réactions émotives des personnes vis-à-vis soit de produits de consommation, soit de programmes de télévision.

lorsqu'il visite un site, peut définir le profil de consommation des internautes et lui enverra la bannière publicitaire adaptée [7].

La participation à des « réseaux sociaux » comme *Linkedin*, *My Space* ou *Facebook* autorise certains « amis », parfois lointains, à exploiter nos données pour des finalités dont nous n'avons pas conscience. Elle invite des sociétés commerciales à utiliser nos données, voire la chaîne de nos amitiés, à des finalités commerciales insoupçonnées [8].

... et pour quoi faire ? Si pour certains traitements, la réponse est évidente même si elle ne l'est peut-être qu'à première vue, pour nombre de traitements, la finalité de l'utilisation des données collectées reste obscure. Ainsi qui eût pensé qu'Amazon, la célèbre librairie américaine en ligne, développe des applications dites d'« *adaptative pricing* », permettant d'adapter automatiquement le prix des ouvrages en fonction de l'élasticité de la demande des internautes, calculée sur la base de méthodes sophistiquées de profilage ? La présence de RFID [9] dans les vêtements des employés peut certes aider à enregistrer de manière plus efficace et facile l'entrée de l'employé dans les locaux de l'entreprise, mais au-delà, permet de tracer le parcours suivi par ce dernier tout au long de la journée et souligner ainsi l'écart présenté par ce trajet par rapport à celui attendu (présence prolongée à la cafeteria, etc.).

Voy. en particulier, M.A. FROOMKIN, « Regulation and Computing and Information Technology. Flood control on the Information Ocean : Living with Anonymity, Digital Cash and distributed Databases, 15, *Journ Law & Com.*, 1996, pp. 395 et s. (cet auteur parle d'un « consommateur myope, mal informé ») ; J. COHEN, « Examined Lives : Informational Privacy and the subject as object », 52 *Stanford Law Journ.*, 2000, pp. 1373 et s.

À propos des multiples applications rendues possibles pour des entreprises à partir des données publiées par nous sur des réseaux sociaux, lire J.P. MOINY, « À propos des réseaux sociaux et de ses enjeux pour la vie privée : le cas *Facebook* », Cahier du CRID, Bruxelles, Bruylant, 2009, à paraître.

Sur les RFID et leurs multiples applications, D. DARQUENNES et Y. POULLET, « RFID : Quelques réflexions introductives à un débat de société, *R.D.T.I.*, janvier 2007, p 255 à 285 ; http://www.strada.be. Les RFID se fondent sur une technologie de l'infiniment petit. L'équipement terminal, c'est-à-dire le microprocesseur qui, tantôt, collectera, traitera, émettra ou recevra les informations ou les communications externes, tantôt, se limitera à l'une ou l'autre de ces opérations, peut voir sa taille réduite à la grosseur d'une tête d'épingle ou d'un grain de sable, à tel point que l'on peut parler de « *Smart Dust* » (poussière intelligente). Ces développements technologiques induisent la possibilité d'interactions largement invisibles entre les « choses » (la souris de l'ordinateur, les marchandises, les vêtements, etc.) ou les personnes sur lesquelles seront implantés ces microprocesseurs et des systèmes d'information qui à partir des informations ainsi collectées et d'autres informations. Cette interaction permettra aux individus porteurs de ces choses d'être aidés dans leur vie de tous les jours à accomplir leurs tâches ou de surveiller leurs activités.

2. De la paranoïa au village global

Ces interrogations doivent-elles mener à l'inquiétude, voire à la paranoïa ? À cette crainte, certains répondent : la transparence n'est-elle pas une vertu, celle qui sied, en tout cas, à l'honnête homme ? À propos de l'Internet, ils évoquent l'analogie avec nos villages traditionnels. Ne parle t'on pas en effet du « village global » [10], métaphore qui est censée nous tranquilliser ! Nos villages traditionnels ne constituent-ils pas des lieux où chacun connaît tout (ou presque tout) de ses voisins souvent pour le meilleur, rarement pour le pire ?

3. Plan

La première partie de l'exposé met à l'épreuve la comparaison esquissée entre les deux types de village. Il en ressort qu'elle est trompeuse. Son examen conduit à ne pas céder trop facilement à l'optimisme béat des bienfaits de la transparence, à laquelle lesdits « réseaux sociaux », les *Facebook*, les *Linkedin*, les *Myspace* nous invitent comme à un jeu gagnant à tous les coups.

Partant de cette comparaison, nous évoquerons les deux facettes de la vie privée et les dangers qu'elle court. Les images du *Big Brother* et du « Procès », empruntées à Solove, un auteur américain [11], nous aideront pour ce faire.

La deuxième partie décrit quelques caractéristiques de l'évolution actuelle des applications des technologies de l'information et de la communication. Au caractère global et convergent des terminaux et des réseaux aux capacités désormais quasi infinies, s'ajoutent désormais deux autres évolutions. La première tient aux applications nouvelles qui trouvent leur traduction dans le web dit 2.0 et le web dit sémantique. La seconde souligne l'omniprésence des systèmes d'information ou leur ubiquité, ce que d'aucuns appellent la naissance des technologies d'« intelligence ambiante ». Deux tendances découlent de cette évolution : la première concerne l'abolissement des

10. « Le village planétaire (en anglais *Global Village*), est une expression de Marshall MCLUHAN, de son ouvrage *The Medium is the Message*, pour qualifier les effets de la mondialisation, des médias et des technologies de l'information et de la communication. Selon ce philosophe et sociologue, « les moyens de communication audiovisuelle modernes (télévision, radio, etc.) et la communication instantanée de l'information mettent en cause la suprématie de l'écrit ». Dans ce monde unifié, l'information véhiculée par les médias de masse fonde l'ensemble des micro-sociétés en une seule. Il n'y aurait selon lui désormais plus qu'une culture, comme si le monde n'était qu'un seul et même village, une seule et même communauté « où l'on vivrait dans un même temps, au même rythme et donc dans un même espace ». Curieux village en vérité, avec des quartiers ne communiquant guère entre eux, traversés de fractures, de frontières, de barrières qui limitent les déplacements des hommes et notamment des pauvres... » (Commentaire repris de Wikipedia, voir Verbo « Village global », http://www.wikipedia.org).
11. D.J. SOLOVE, *The Digital Person*, New York University Press, New York and London, 2004.

frontières entre espaces public et privé ; la seconde, la responsabilité dite « globale » de chaque acteur, ce qui nous amènera à une réflexion sur l'intérêt d'introduire en droit des technologies de l'information et de la communication certains concepts et certains principes du droit de l'environnement.

Ces réflexions amènent dans une troisième partie à s'interroger sur la nécessité de repenser, de « réinventer » nos législations de protection des données. Cette réflexion s'appuie sur une analyse de la directive 2002/58/C.E. concernant le traitement de données et la protection de la vie privée dans le secteur des communications électroniques, qualifiée de directive e-privacy [12]. Cette directive en cours de révision [13] introduit, de manière subreptice mais certaine, des dispositions qui vont bien au-delà du champ d'application de la directive 95/46/C.E. et de nos législations classiques en matière de protection des données à caractère personnel et dès lors indiquent la nécessité de législations « Vie privée » de troisième génération. Au-delà, nous rappellerons quelques grands principes à l'aune desquels les développements récents de la société de l'information doivent être appréciés si nous souhaitons la survie de nos libertés. La protection de la vie privée ne constitue-t-elle pas la condition indispensable de cette survie, voire de la survie de nos sociétés démocratiques ?

12. *J.O.C.E.*, 31 juillet 2002, L.201, pp. 37 à 47.
13. Et ce dans le cadre de la révision du cadre réglementaire pour les réseaux et services de communication électronique (*Review of the Telecom Package*). Le 13 novembre 2007, la Commission adoptait dans ce contexte une proposition de modification du texte de la directive. Une position commune du Parlement et du Conseil a été adoptée en date du 27 novembre 2008. Le texte de la proposition modifié suite à la position commune (Proposition amendée pour une directive du Parlement européen et du Conseil modifiant la directive 2002/22/C.E. sur le service universel et les droits des utilisateurs des réseaux de communications électroniques et la directive 2002/58/C.E. relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (COM (2007)2008 – C6-0430/2007 -2007/0248(COD)) sera débattu en seconde lecture devant le Parlement européen au mois de mars. Sur ces textes, voir les deux avis du Contrôleur européen de la protection des données sur la révision de la directive 2002/58/C.E. relatif à la protection des données en date du 10 avril 2008 et tout récemment du 9 janvier 2009 (ces avis sont publiés sur le site du Contrôleur : http://www.edps.europa.eu).

SECTION 1

Qu'est-ce que la vie privée ? - Leçons des enseignements de Kafka et d'Orwell

A. La comparaison trompeuse avec le village traditionnel

4. De la non-transparence de l'individu comme vertu

Reprenons la comparaison esquissée dans l'introduction. Notre village « global » fonctionne-t-il comme nos villages anciens ? On note que dans le village ancien, la connaissance que chacun donne à d'autrui se heurte à une limite : entre les quatre murs de ma maison, je suis chez moi. Cet espace privé est inviolable. Il est vital pour me permettre de me ressourcer à l'ombre ou caché du regard d'autrui. De même, le droit se doit de protéger la communication privée que j'entretiens avec autrui. Cette préoccupation justifie la première conception de notre droit à la vie privée, tel que consacré par l'article 8 de la Convention européenne des droits de l'Homme, dès 1950 [14].

Des moments de « discrétion, d'anonymat et de solitude », ou encore « de repli et de dissimulation » [15] sont en effet nécessaires à la réflexion et à la capacité, pour l'individu, de remettre en question ses choix, de développer des relations significatives à autrui. L'amitié et l'amour ne s'expriment pas facilement en public ; ils demandent le recul et l'isolement sélectifs. Déjà dans les villages traditionnels, le rôle joué par les murs des habitations privées était de protéger une sphère d'intimité dans laquelle les individus se sentaient libres d'abandonner le rôle qu'ils endossaient en public, le temps de leurs activités privées.

C'est en ce sens que « le droit à l'opacité » est une condition nécessaire à toute recherche d'« authenticité » vis-à-vis de soi-même et dans ses rapports avec autrui. La nécessité de garantir cette opacité s'explique par le besoin de reconnaître à chacun des lieux où, en tant qu'être humain, il peut développer sa personnalité [16].

14. La conception originaire du droit au respect de la vie privée faisait découler ce droit du principe du respect dû à la dignité humaine et en faisait une condition du libre développement de la personnalité : la protection de l'intimité familiale et domestique, entre les murs du domicile – lieu « privé » s'il en est – et de la correspondance.
15. R. GAVISON, « Privacy and the limits of Law », 89 *Yale Law Journal*, 1980, pp. 433 et s.
16. Voy. sur cette problématique les réflexions de J. RAYMAN (« Driving to the Panopticon : A Philosophical Exploration of the Risks to Privacy Posed by the Highway of the Future », 11 *Santa Clara Computer & Techn. Law Journal*, 1995, pp. 22 et s.) ; J. COHEN (« Examined Lives : Informational Privacy and the Subject as Object », 52 *Stanford Law Rev.*, 2000, pp. 1373 et s.) et H. NISSENBAUM (« Privacy as contextual Integrity », 79 *George. Washington Law Rev.*, 2004, pp. 150 et s.), qui affirment que « l'absence d'examen et de zones de "relatives étroitesses de vues" sont les conditions nécessaires pour formuler des objectifs, des valeurs, des conceptions de soi et des principes d'action parce qu'elles constituent des lieux dans lesquels les personnes sont libres d'expérimenter, d'agir et de décider sans rendre compte aux autres et sans craindre de sanctions » (traduction libre).

Tel que nous l'aborderons ci-après (*infra* n° 9), ce « droit à l'isolement » semble être aujourd'hui dans notre société moderne encore plus vital que jamais et justifie la mise en place de nouveaux instruments législatifs pour protéger « l'opacité des individus » contre les nouveaux défis technologiques et sociopolitiques actuels.

5. De la vertu d'opacité singulièrement mise à mal

Or, cette nécessité de garantir à chacun une certaine « opacité » est, dans nos sociétés de l'information, mise à mal au moment où les murs de nos maisons ne nous cachent plus du regard d'autrui.

Sans doute, peut-on évoquer à ce propos les systèmes de surveillance infrarouges que les armées ou polices peuvent utiliser pour détecter la présence et les mouvements à l'intérieur des bâtiments mais, au-delà, les technologies de l'information et de la communication s'avèrent bien plus envahissantes encore.

Ainsi, des RFID, insérées dans nos habits, dans nos produits de consommation (couplées par exemple avec le frigo intelligent) et appareils électroniques, voire dans nos corps, informent les destinataires des messages situés au-delà des murs de nos maisons avertis par les réseaux qu'empruntent les messages captés à partir ou émis par ces « puces », de nos actions parfois les plus triviales comme boire notre jus de fruit favori, notre état de stress au réveil [17], nos déplacements [18].

Autre exemple plus évident encore, toutes nos utilisations de notre navigateur sont révélées au moins à notre fournisseur d'accès. Il peut savoir quelles pages nous avons lues, quelles informations nous avons cherchées, quels produits ou services nous avons consommés ou allons consommer [19].

17. Sur les applications de suivi médical et les implants TIC dans le corps des individus, lire l'avis du Groupe européen d'Éthique des sciences et des nouvelles technologies auprès de la Commission européenne, « *Aspects éthiques des implants TIC dans le corps humain* », 16 mars 2005.
18. Sur les applications des RFID et autres technologies de l'intelligence ambiante, lire A. GREENFIELD, *Every(ware), la révolution de l'ubimédia*, FYP Editions, Limoges.
19. La question de la surveillance des consommateurs et de leur comportement en ligne a fait l'objet de nombreux rapports et discussions au sein de la FTC (Federal Trade Commission) américaine, voir notamment le rapport et les discussions relatives à l'« Online Behavioral Advertising Moving the Discussion Forward to Possible Selfregulatory Princples », disponible sur le site : http://www.ftc.gov.bcp/ avec le débat tenu les 1 et 2 novembre 2007 sur le thème : « Behavioral Advertising : Tracking, Targeting and Technology ». Voir également *World Privacy Forum, The Network Advertising Initiative : Falling at Consumer Protection and Selfregulation*, document publié le 2 nov. 2007 sur le site : http://www.worldprivacyforum.org.

Enfin, l'exemple de Gmail [20] en témoigne, notre serveur de courrier électronique peut repérer dans notre correspondance les mots clés qui la ponctuent [21].

Bref, nous voilà en permanence surveillés, épiés au-delà des zones que jusqu'à présent nous considérions comme inviolables.

6. ... à la nécessité d'une maîtrise de notre environnement

Une seconde différence tient à la maîtrise, sans doute toute relative mais certaine, que nous avons dans nos villages traditionnels de la circulation de notre image informelle. Nous savons, ou en tout cas nous devinons, que notre rentrée tardive ou sortie matinale, notre changement de costume ou de voiture, l'acquisition ou au contraire la perte de notre emploi, tous ces événements auront telle répercussion suivant tel circuit de communication, depuis la voisine malveillante jusqu'à l'ami qui nous téléphonera le soir pour nous féliciter ou nous plaindre. Nous pouvons, en fonction de cela, adapter notre comportement, jouer tel ou tel personnage, cacher certains choix. Dans cette mesure, nous maîtrisons notre environnement. Qu'en est-il dans notre village global ? Avons-nous la même maîtrise ? Incontestablement non !

En témoignent ces technologies dites du *one to one marketing* ou de l'*adaptative pricing*, par lesquelles certains opérateurs en fonction de la connaissance prédictive qu'ils déduisent de notre profil, tantôt (*adaptative pricing*) nous affichent le prix qui tient compte de notre « appétit » d'achat supposé quant à ce bien, tantôt (*one to one marketing*) nous affichent la publicité la plus adaptée à notre comportement de consommateur [22].

Ces applications sont fondées sur l'adoption des techniques de profilage que nous abordons maintenant.

7. Les techniques de profilage

Ces techniques utilisent des méthodes statistiques qui, à partir de croisements aléatoires de données figurant dans de larges entrepôts de données (les *datawarehouses*), infèrent à propos d'un individu des comportements types liés à l'appartenance à un groupe ou plutôt à un profil [23].

Ainsi, l'agrégation de données en provenance de diverses bases de données permettra de déduire avec un taux de 89 % de certitude que la composition de tel panier d'achat par un consommateur se présentant dans une grande surface à telle heure de la journée induit le fait que cette personne est vraisemblablement célibataire, amateur de voyages lointains et fraudeur potentiel. Le profil du terroriste se déduit du croisement de données aussi diverses que le registre de population, les utilisations de cartes de crédit, les déplacements recensés grâce aux mobilophones, les cartes de fidélité, la consommation de médicaments, etc. [24]. La diminution drastique des coûts de stockage, la sophistication des outils d'analyse de données et les puissances de calcul des serveurs autorisent ces croisements aléatoires d'où sortent la vérité au moins statistique des profils qu'il reste à confronter aux données relatives à des personnes particulières. Bref, le citoyen se voit appliquer le résultat d'une connaissance déduite de ce profil construit à partir de données qui ne le concernent pas, qui ont souvent peu de lien logique avec l'opération pour laquelle ce profil est utilisé et qui lui sont largement inconnues.

Pire, ce profil induit pour le responsable du traitement une meilleure connaissance de la personne concernée que celle que ce dernier pourrait avoir de lui-même et si cette personne conteste l'exactitude de ce profil ou en tout cas que la décision prise à son égard est erronée, il lui appartiendra de faire la preuve de cette erreur [25].

8. Les réseaux sociaux

Pour avoir lu de près les *privacy settings* de *Facebook* ou autres réseaux sociaux et opéré en connaissance de cause les restrictions à la diffusion des informations

20. http://mail.google.com/mail/help/intl/fr/privacy.html.
21. À cet égard, l'analyse dressée par le Groupe dit de l'article 29 des services de criblage de courrier électronique, qui permettent automatiquement à partir de mots clés repérés dans les messages envoyés ou reçus par nos ordinateurs de détecter la signification de ceux-ci aux motifs, louables selon leur concepteur, de lutter contre les courriers non sollicités ou de prévenir des actes illicites, mais au grand dam du principe du secret de la correspondance qu'elle soit électronique ou non (Avis 2/2006 du groupe de travail de l'article 29 sur les questions de protection de la vie privée liées à la fourniture de service de criblage des courriels, 21 février 2006, WP.118) et même à des fins de corrélation des données entre les différents services du moteur de recherche ou de tiers (Avis 1/2008 du groupe de travail de l'article 29 sur les aspects de la protection des données liés aux moteurs de recherche, 4 avril, WP.148).
22. On note que cette dernière pratique transforme la conception d'une publicité comme ouverture à (ou de tentations vers) des mondes inconnus en celle d'une simple confirmation des choix antérieurs du consommateur.
23. Sur les décisions prises sur la base de profilages des individus, profilages issus d'opérations de « *data mining* » (forage de données) et leur importance dans la prise de décisions des administrations et des entreprises, lire J.M. DINANT, C. LAZARO, Y. POULLET, A. ROUVROY, Rapport au Comité consultatif « Convention n° 108 » du Conseil de l'Europe, Septembre 2008, disponible sur le site du Conseil de l'Europe http://www.coe.int/. Voir également, l'excellent ouvrage rassemblant des articles sur le thème du profilage, édité par M. HILDEBRANDT et S. GUTWIRTH, *Profiling the European citizen, Cross disciplinary Perspectives, Springer Science*, Dordrecht, Pays Bas et N. LEFEVER et Y. POULLET, « Entrepôts de données et vie privée », *R.D.T.I.*, 2008/30, pp. 7-20, http://www.strada.be.
24. À propos des applications du *data mining*, en matière de sécurité publique, lire D.J. SOLOVE, « Data Mining and The Security – Liberty Debate, 75 *University Chicago Law Review*, 2008, pp. 343 et s. L'auteur évoque en particulier le programme américain MATRIX (*Multistate Anti-Terrorism Information Exchange*).
25. Sur ce renversement de la preuve induit par le profilage, lire D.J. STEINBOCK, Data Matching, Data Mining and Due Process, 40 *GA Law Rev*, (2005), 1, pp. 82 et s.

qui nous concernent au cercle choisi, nous pensons maîtriser parfaitement la circulation de notre image informationnelle. Un coup d'œil sur les *privacy notices* de ces opérateurs [26] ébranle cependant cette assurance. La publicité qui nous est adressée parce que nous figurons comme amis de telle ou telle personne et donc devons comme lui y être sensible, la rétention de nos données au-delà de la résiliation de notre contrat avec l'opérateur de socialisation, autant d'exemples qui attestent de la maîtrise bien incomplète de nos données.

9. Les deux facettes de la vie privée [27]

Bref, un individu de plus en plus transparent et opérant dans un monde virtuel au fonctionnement de plus en plus opaque. Voilà ce que révèle l'analyse des pratiques des opérateurs sur l'Internet. Elle renvoie aux deux facettes de notre vie privée et que nos législations de protection des données à caractère personnel entendent garantir.

La protection des données, si elle consacre des droits subjectifs nouveaux, trouve bien son fondement dans les préoccupations qui sont à la base de la notion de vie privée.

Ces législations entendent en effet consacrer, d'une part, le droit à l'intimité ou plus largement le droit de se retirer de la société et d'autre part, celui d'y développer ses propres choix. Ces deux acceptions de la notion de *privacy* ne sont pas incompatibles entre elles, bien au contraire. Elles traduisent un objectif commun : permettre à l'individu de participer pleinement à la vie sociale. La réalisation de cet objectif suppose, à la fois, le « droit à la séclusion » ou plutôt la liberté de ne pas être exposé (le « droit » de ne pas participer à la société de l'information), condition structurelle de l'évolution de l'Homme dans la mesure où elle permet l'autonomie réflexive et la liberté de définir, et partant de choisir, son mode d'existence et de relation à autrui et, à la fois, le « droit à participer pleinement à une société démocratique de l'information en contrôlant la circulation de son image informationnelle et ses usages ».

On note que ces deux acceptions sont intimement liées et s'arc boutent l'une à l'autre : la première est condition de la seconde dans la mesure où elle permet à l'individu de construire son autonomie et son identité afin dans un second temps, de s'affirmer dans la société (la *privacy* comme condition de la liberté d'expression) et de veiller au respect de ses libertés par une maîtrise des flux informationnels qui l'entourent (contrôle du pouvoir informationnel d'autrui) afin notamment que soit garanti son droit à la séclusion (effet retour de la seconde acception sur la première : nous ne pouvons participer en toute quiétude à la société de l'information que si on nous garantit au moins partiellement l'opacité (par exemple, par la possibilité de recourir à l'anonymat ou au pseudonyme, par la possibilité de désactiver les terminaux qui permettent de nous localiser), qui est une condition de notre liberté).

Ces deux facettes sont mises à mal. Deux « figures » tirées de romans célèbres permettent, selon Solove [28], d'illustrer la manière dont les technologies affaiblissent le droit à la vie privée et modifient en profondeur les relations entre les responsables de traitement et les personnes concernées.

B. La société de l'information : entre le jugement de Kafka et le *Big Brother* d'Orwell

10. *Big Brother*

La première figure proposée par Solove est celle du *Big Brother* de G. Orwell dans son célèbre ouvrage « 1984 ». Cette première référence entend traduire la puissance que le traitement de l'information donne dans nos sociétés aux responsables du traitement face à des personnes concernées, qu'elles soient citoyennes, employées ou consommateurs, de plus en plus transparentes au regard de ce *Big Brother* qui entend normaliser nos comportements pour notre bien à chacun. L'information représente pour ceux qui la détiennent un pouvoir vis-à-vis de ceux sur lesquels l'information est détenue. Celui qui détient l'information sur autrui peut adapter sa décision en fonction de la connaissance que l'information collectée et traitée lui donne d'autrui. Il prévoit son attitude et peut donc répondre à sa demande ou influencer celle-ci.

Sans doute, et nous reviendrons sur ce point (*infra*, n° 38), est-il urgent de rétablir, par des droits nouveaux, une certaine symétrie informationnelle sous peine de voir celui à propos duquel on sait tout, se transformer en un simple objet de domination. Ainsi, on s'inquiète à juste titre de la puissance que confèrent ou peut conférer à *Google* diverses activités qu'il mène par lui-même ou des membres de son groupe.

On ose à peine imaginer la connaissance de chacun que *Google, big brother* de nos temps modernes, peut collecter, croiser et ainsi déduire de l'utilisation combinée ou non d'applications comme son moteur de recherche (*Google*

26. Voy. par exemple http://fr-fr.facebook.com/policy.php?ref=pf.

27. Sur ces deux facettes de la vie privée et leur lien intrinsèque, A. ROUVROY et Y. POULLET, « The right to informational self-determination and the value of self-development – Reassessing the importance of privacy for democracy, in Reinventing Data Protection, Proceedings of the Colloquium held at Brussels », Nov 2007, *Springer Verlag*, 2009. *Cf.* également, mais en fondant ces deux facettes sur la première, la vie privée et l'autre, le droit à la protection des données, P. DE HERT and S.GUTWIRTH, « Privacy, Data Protection and law enforcement. Opacity of the individuals and Transparency of the power », *in Privacy and the Criminal Law*, E.CLAES *et alii* (ed.), Interscientia, Antwerpen-Oxford, 2006, p. 74.

28. D.J. SOLOVE, *The Digital Person*, New York University Press, New York and London, 2004.

Search Engine), son service de courrier électronique (G-mail), ses services d'information en ligne (*Google News*), ses services d'information géographique (*Google Earth et Google Maps*, désormais couplé avec *Google Latitude*) et les services de publicité en ligne développés par sa filiale DoubleClick qui, grâce à sa technologie des hyperliens invisibles, récolte les données de navigation des millions d'internautes auprès de milliers de sites web connectés à Double-click.

11. « Le Procès » (*Der Prozeß*)

La seconde figure est celle du Procès de F. Kafka, un ouvrage de 1925. En résumé, une personne est l'objet d'un procès dont elle ignore le plaignant, la raison du procès tout comme les griefs qui lui sont adressés.

La référence amène ici à s'interroger sur l'opacité des systèmes qui nous entourent, dont nous ignorons le plus souvent l'exacte finalité, les réels destinataires et l'ampleur. Cette opacité peut conduire à une certaine crainte vis-à-vis d'un tel environnement et l'adoption d'un comportement le plus conforme à la norme que nous jugeons être celle attendue par autrui, le responsable du traitement. Des psychologues ont ainsi démontré que nos comportements s'infléchissent et que, dans des contextes où nous nous savons, voire croyons, être épiés, les mouvements spontanés de joie et de colère n'osent plus s'exprimer, sans doute refoulés vers d'autres lieux, ce qui n'est pas nécessairement meilleur.

C. La décision du Tribunal constitutionnel allemand sur le recensement de 1983[29] : l'importance fondamentale de la vie privée pour nos démocraties

12. De la consécration du droit à l'autodétermination informationnelle

Dans la même ligne que celle dénoncée par Kafka, une des premières décisions d'une cour constitutionnelle consacrant le droit à la protection des données, celle du Tribunal constitutionnel allemand de 1983[30], relevait précisément à

29. Tribunal constitutionnel fédéral de Karlsruhe, 15 décembre1983, *EuGRZ*, 1983, pp. 588 et s. Sur cette décision, voy. E.H. RIEDL, « New bearings in German Data Protection », *Human Rights Law Journal*, 1984, Vol. 5, n° 1, pp. 67 et s ; H. BURKERT, « Le jugement du Tribunal constitutionnel fédéral allemand sur le recensement démographique et ses conséquences », *Dr. Inf.*, 1985, pp. 8 et s. Voy. aussi E. BROUWER, *Digital Borders and Real Rights*, Nijmegen, Wolf Legal Pub, 2007. Le 27 février 2008 le Tribunal constitutionnel fédéral allemand rappelait cette décision et, sur la base du même raisonnement, proclamait un droit constitutionnel nouveau : « le droit à la garantie de la confidentialité et de l'intégrité des systèmes d'information » (« Das Recht auf gewährleistung der vertraulichkheit und integrität informationtechnischer Systeme »). Sur cette décision, nos commentaires, *infra*, n° 35.
BVerfGE 65, 1 – Volkszählung Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983-1 BvR 209, 269, 362, 420, 440, 484/83 in

propos d'une loi de recensement votée pourtant à l'unanimité, nombre de manquements : l'absence de définitions claires des objectifs poursuivis, le manque de transparence des circuits que suivaient les informations collectées lors du recensement et l'information déficiente procurée aux citoyens allemands. Ces lacunes constituent, selon le Tribunal, une atteinte à la dignité humaine et au libre développement de la personnalité. Le Tribunal fédéral soulignait les conséquences dangereuses pour la démocratie de ces traitements au fonctionnement opaque.

En particulier, il mettait en évidence les restrictions que les individus s'imposent automatiquement, voire inconsciemment, et leur crainte d'adopter des comportements qui seraient considérés comme déviants ou simplement étranges, par les tiers[31].

Le tribunal souligne la crainte des personnes, dans la mesure où ces comportements seraient révélés à autrui, que puissent s'en suivre des conséquences défavorables.

En conclusion, le Tribunal fédéral estime que le développement technologique risque : « de détruire, non seulement nos chances de nous développer mais aussi le bien-être commun (*Gemeinwohl*), car l'autodétermination est la condition fonctionnelle élémentaire d'une communauté démocratique libre fondée sur la capacité des citoyens d'agir et de coopérer »[32].

den Verfahren über die Verfassungsbeschwerden. À propos du raisonnement tenu par la Cour et son actualité, lire Y. POULLET et A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel – Une réévaluation de l'importance de la vie privée pour la démocratie », *in État de droit et virtualité*, Actes du colloque organisé à Montréal par la Chaire L.J. Wilson, octobre 2007, à paraître.

31. « Les possibilités d'inspecter et de gagner en influence ont augmenté à un point jamais atteint auparavant et pourraient influencer le comportement des individus en raison de la pression psychologique exercée par les intérêts publics. Même sous certaines conditions de technologies modernes du traitement de l'information, l'autodétermination individuelle présuppose que l'individu continue à disposer de sa liberté de décider d'agir ou de s'abstenir, et de la possibilité de suivre cette décision en pratique. Si l'individu ne sait pas prévoir avec suffisamment de certitude quelles informations le concernant sont connues du milieu social et à qui celles-ci pourraient être communiquées, sa liberté de faire des projets ou de décider sans être soumis à aucune pression est fortement limitée. Si l'individu ne sait pas si un comportement déviant est remarqué et enregistré de façon permanente en tant qu'information, il essaiera de ne pas attirer l'attention sur un tel comportement. S'il craint que la participation à une assemblée ou à une initiative des citoyens soit officiellement enregistrée et qu'il coure personnellement des risques en raison de cette participation, il renoncera probablement à l'exercice de ses droits. Ceci n'a pas seulement un impact sur ses chances de se développer, le Bien-être commun (*Gemeinwohl*) en est aussi affecté car l'autodétermination est une condition élémentaire fonctionnelle dans une société démocratique libre, basée sur la capacité des citoyens d'agir et de coopérer ». (traduction libre).

32. La Cour allemande ajoute : « La valeur et la dignité de la personne fondées sur l'autodétermination de celle-ci en tant que membre d'une société libre constituent la pierre angulaire de l'ordre établi par la Loi fondamentale. Le droit général à la personnalité consacré aux articles 2 (1) et 1 (1) GG protège ces valeurs (...). »

13. ... à la démocratie

C'est à la lumière de cette réflexion que doit se concevoir aujourd'hui l'importance des règles entourant la vie privée et garantissant la protection des données. Ces régimes apparaissent nécessaires par le soutien qu'ils apportent aux individus pour sauvegarder ou développer leurs capacités d'autonomie à agir et à coopérer à l'intérieur d'une société qui puisse ainsi rester démocratique car fondée sur le respect des différences et le libre développement de chacun [33].

Cette décision constitutionnelle allemande, suivie point par point par une autre décision récente prise par le même tribunal, à propos d'une loi permettant l'intrusion policière à distance dans les ordinateurs [34], atteste du caractère fondamental de la protection de la vie privée conçue comme droit à l'autodétermination informelle et condition d'une véritable démocratie délibérative [35], c'est-à-dire d'un État respectueux du développement orignal de chacun mais au-delà comme condition des autres libertés démocratiques [36]. Ainsi peut-on envisager une véritable liberté d'expression si chacun se sait observé dans ses choix et activités ?

Peut-on imaginer une complète liberté de déplacement, dans un monde où le mobilophone, le cas échéant RFID ou GPS aidant, permet de suivre nos moindres déplacements et de nous alerter sur la présence de tel ou tel événement ? La vie privée, dont les lois de protection des données à caractère personnel garantissent désormais l'exercice effectif, constitue ainsi « la » liberté fondamentale, en tant qu'elle conditionne la survie des autres libertés [37].

33. Sur ce point, lire S. GUTWIRTH et P. DE HERT, « Regulating Profiling in a democratic constitutional State », *in* M. HILDEBRANDT et S. GUTWIRTH, *Profiling the European citizen, Cross disciplinary Perspectives*, Springer Science, Dordrecht, Pays Bas.
34. Le 27 février 2008, le Tribunal constitutionnel allemand (décision publiée *in* MMR, 2008, 303 avec note critique de T. HOEREN (MMR, 2008, 366) ; *R.D.T.I.*, 2009/34, http://www.strada. be avec note de P. DE HERT, K. de VRIES et S. GUTWIRTH) devait consacrer, en suivant la même argumentation que celle de 1983, un « Recht auf Gewährleistung der Integrität und Verbrauchlichkeit informationstechnischer System » (Sur cette décision nos remarques, *infra*, n° 35).
35. Le lien entre la vie privée, condition de l'expression libre, originale et respectueuse des différences et la démocratie est développé par de nombreux auteurs, ainsi Jürgen HABERMAS, *Between Facts and Norms*, MIT Press, 1996 ; P.M. SCHWARTZ, et W.M. TREANOR, « The New Privacy », *Michigan Law Review*, 101, 2003, p. 216 ; James E. FLEMMING, « Securing Deliberative Autonomy », *Stanford Law Review*, Vol. 48, N.1, 1995, pp. 1-71, qui soutient que la structure de base de l'autonomie délibérative garantit les libertés fondamentales qui sont des conditions préalables significatives à l'habilité des personnes à délibérer et à prendre certaines décisions fondamentales qui affectent leur destin, leur identité ou leur mode de vie. Sur la démocratie délibérative, voy., James E. FLEMMING, « Securing Deliberative Democracy », *Fordham Law Review*, Vol. 72, p. 1435, 2004.
36. Sur le lien entre la protection de la vie privée « psychique » et la liberté d'expression, lire N. M. RICHARDS, « Intellectual Privacy », vol. 87, n° 2, *Texas L. Rev*, décembre 2008.
37. H. BURKERT, « Dualities of Privacy -An Introduction to "Personal Data Protection and Fundamental Rights" », *dans Privacy- New visions*, M.V. Perez et A. Palazzi (eds), Cahier du Crid, 2008, pp. 14-25.

SECTION 2

De quelques caractéristiques des applications des technologies récentes de l'information et de la communication

14. De nouvelles technologies... de nouveaux risques pour la vie privée

Cette assertion de la valeur fondamentale de notre vie privée nous conduit à jeter un œil sur les caractéristiques des technologies nouvelles pour en saisir les implications sur nos comportements et par là, notre vie privée, conçue comme capacité d'épanouissement. Les lois de protection des données à caractère personnel du type européen entendaient répondre aux risques générés par les traitements de l'information, que nous connaissions en 1995.

Loin de nous l'idée que les concepts mis alors en place, à l'aube de la révolution de l'Internet, ne constituent pas encore aujourd'hui les éléments de base de la protection de nos libertés. Il n'empêche : la révolution de l'Internet, la convergence des réseaux, l'accroissement de puissance tant de stockage que de traitement des terminaux et l'intelligence ambiante doivent nous amener à imaginer une nouvelle approche ou du moins des moyens complémentaires qui permettent d'assurer une protection actualisée, effective et adéquate de notre vie privée. Sans doute, le facteur technologique n'est pas le seul à prendre en considération pour décrire les nouveaux risques encourus. Contrairement à ce que suggère notamment Lessig [38], l'évolution technologique n'est pas la seule raison pour laquelle il convient d'adapter notre cadre législatif.

L'évolution des circonstances socio-politiques, ainsi le cauchemar du 11 septembre 2001 et ses suites [39], peuvent elles aussi générer de nouvelles

38. L. LESSIG, *Code and other Laws of Cyberspace*, New York, Basic Book, 2000. Pour de plus amples réflexions sur la manière dont la révolution Internet et plus récemment, les technologies d'Intelligence Ambiante métamorphosent les risques que courent les individus et leurs droits fondamentaux et sur l'appel à de nouvelles actions législatives visant à renforcer les différentes facettes identifiées de la vie privée, voy. A. ROUVROY, « Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence », *Studies in Ethics, Law, and Technology*, Berkeley Electronic Press, 2008.
39. À cet égard, l'ouvrage de Juge R. POSNER qui justifie les atteintes répétées à la vie privée dues à la lutte antiterroriste : « *Not a suicide Pact : The Constitution in a Time of National Emergency* », Oxford Univ. Press., 2006. L'auteur écrit notamment « En cas de doute sur les conséquences vraisemblables et réelles d'une mesure (de surveillance), le juge pragmatique et empirique sera incliné à donner la primauté aux décisions des autres branches du gouvernement... Les juges ne sont pas supposés en connaître beaucoup à propos de sûreté nationale. » (traduction libre). *Cf.* également, E.A. POSNER et A.VERMEULE (*Terror in the Balance : Security, Liberty and the Courts*, Oxford Univ. Press, 2007) qui estiment que « les droits constitutionnels doivent s'effacer de telle manière que l'exécutif puisse de manière décidée lutter contre les atteintes et dangers. » (traduction libre).

menaces pour l'autodétermination des personnes, et l'adaptation des législations de protection des données à caractère personnel et des multiples facettes de la vie privée peut s'avérer cruciale à cet égard également.

Les lois garantissant le respect de la vie privée et mettant en œuvre la protection des données doivent donc être adaptées en fonction des évolutions technologiques économiques et socio-politiques qui menacent les conditions nécessaires aux individus pour développer leur capacité à développer librement leur personnalité.

15. Trois évolutions majeures

Le développement des technologies de l'information peut se laisser décrire, chronologiquement, comme la succession de trois évolutions : la première, connue sous le nom de « loi de Moore », consiste en l'accroissement continu des capacités des ordinateurs, des terminaux et des infrastructures de communication, à laquelle s'ajoute la puissance quasi infinie de traitement lié aux fonctionnement des systèmes d'information. La deuxième coïncide avec la « révolution de l'Internet », qui se décline en différents aspects : ainsi premièrement, la convergence des réseaux autour d'une norme unique permettant une totale interopérabilité ; en deuxième lieu, l'apparition du web dit « sémantique », du web 2.0 et enfin, l'évolution des techniques d'identification et d'authentification. Enfin, la troisième consiste en une révolution plus profonde encore, celle de l'« intelligence ambiante » qui met la technologie et le réseau au cœur du réel : des objets qui nous entourent, des lieux que nous fréquentons et des corps que nous habitons.

16. Deux tendances induites

Cette évolution technologique favorise deux tendances lourdes de nos activités sur la toile : la première souligne une privatisation de ce cyberespace, non seulement encadré par des normes qui émanent de pouvoirs privés mais également dont l'accès est soumis aux lois de ceux qui détiennent l'information posant ainsi la question de l'accès au savoir et à la connaissance ; la seconde constate la portée globale de nos actions sur l'Internet et la façon dont le fonctionnement de nos terminaux et de l'infrastructure modèle nos comportements et nos interactions [40]. Cette seconde observation conduit à reconnaître une certaine responsabilité des opérateurs et constructeurs de terminaux en ce qui concerne notre environnement communicationnel et appelle quelques

40. C'est toute la thèse de LESSIG qui voit dans la technologie une méthode de régulation au même titre que la loi et souvent plus efficace que cette dernière (*Code and other Laws of Cyberspace*, New York, Basic Books, 2000).

considérations sur une possible application dans le domaine de la réglementation de protection des données des principes du droit de l'environnement.

A. Trois évolutions majeures

1. *L'accroissement des capacités de stockage, traitement et transmission de même que l'évolution des équipements terminaux*

17. La loi de Moore

La première évolution concerne les supports d'information. Il est coutumier à leur propos de rappeler la loi de Moore qui établit que la performance des supports d'information double tous les dix-huit mois (soit par mille tous les quinze ans) alors que, dans le même temps le prix diminue de moitié pour une performance égale.

Dans une étude réalisée pour le Conseil de l'Europe sur les défis nouveaux rencontrés par la protection des données [41], nous concluions : « il est devenu et il deviendra de plus en plus possible et de moins en moins cher d'enregistrer la vie de tous les individus de la planète (la nôtre et celle des autres...) [42] ».

À titre d'illustration, nous pouvons examiner la faisabilité de l'enregistrement de toutes les communications téléphoniques sortant d'Europe vers le monde entier. Ce n'est pas rien puisqu'il s'agit de stocker l'équivalent de cinquante milliards de minutes de télécommunications vocales [43] sur une base annuelle [44].

41. Y. POULLET et J.M. DINANT, « L'autodétermination informationnelle à l'ère de l'Internet », Éléments de réflexion sur la Convention n° 108 destiné au travail futur du Comité consultatif (T-PD), Rapport publié sur le site du Conseil de l'Europe, http://www.coe.int/T/F/Affaires%5Fjuridiques/Coop%E9ration%5Fjuridique/Protection%5Fdes%5Fdonn%E9es/.

42. Cette augmentation explique que désormais enregistrer tous les faits et gestes de la vie d'un individu n'est plus chose impossible avec un ordinateur personnel. L'expérience, baptisée « *LifeLog* », qui consiste en l'enregistrement de la totalité des événements, expériences et interactions d'une personne avec le monde qui l'entoure, est d'ailleurs en cours dans le cadre d'un projet de *l'Information Processing Technology Office* (IPTO), une agence de la *Defense Advanced Research Projects Agency* américaine.

43. Calcul réalisé sur la base d'une extrapolation des chiffres fournis par l'Union Internationale des Télécommunications pour l'année 1999 (vu sur : http://www.itu.int/ITU-D/ict/statistics/atglance/Eurostat 2001.pdf).

44. En 1980, cela eût nécessité au bas mot des millions d'enregistreurs avec autant de bandes magnétiques. À cette époque, il fallait un enregistreur pour enregistrer une conversation.

Si l'on considère qu'il faut environ dix mille bits par seconde pour digitaliser la voix et que l'on peut comprimer les données d'un facteur deux (ce qui est classique), on observe qu'il faudra en moyenne de l'ordre de cinq téra-octets pour stocker 24 heures de trafic, ce qui à l'heure actuelle est tout à fait envisageable avec des systèmes de *disk array* où chaque disque peut stocker de l'ordre de 400 giga-octets [45].

En outre, le débit moyen de ce flux continu de centaines de milliers de communications simultanées représente un débit d'environ 0,5 gigabits par seconde, ce qui est largement supportable par une seule fibre optique de l'épaisseur d'un cheveu [46]. En d'autres termes, il serait techniquement possible de faire passer TOUT ce trafic téléphonique à travers un mince tube en verre de quelques microns d'épaisseur.

Dans le commerce, on trouve actuellement des systèmes de type walkman capables d'enregistrer le contenu de l'équivalent de plusieurs centaines de CD-ROM classiques au format MP3. Les appareils photos digitaux permettent de stocker des centaines, voire des milliers de photos alors que la capacité du film classique plafonne à 36 vues.

Cette augmentation des capacités de stockage, de traitement et de transmission explique qu'en quelques secondes, *Google* puisse traiter votre demande, scannant plus de 500.000 sites dans le monde.

18. Les équipements terminaux : de la multifonctionnalité à la miniaturisation

Une deuxième évolution notable affecte les équipements terminaux. L'évolution est multiple. Elle est bien évidemment technique, d'ordre fonctionnel, ensuite et concerne leur réglementation, enfin.

La notion de « terminal » est définie par la directive européenne sur les équipements terminaux [47] de la façon suivante : « un produit permettant la communication, ou un composant pertinent d'un produit, destiné à être connecté directement ou indirectement par un quelconque moyen à des interfaces de réseaux publics de télécommunications (à savoir des réseaux de télécommunications servant entièrement ou en partie à la fourniture de services de télécommunications accessibles au public) ».

45. Voir, par exemple sur www.hitachi.com le 400GB Deskstar 7K400.
46. Actuellement, des débits de 2,5 à 10 gigabits par seconde sont classiques sur ce type de support.
47. Directive 1999/5/C.E. du Parlement européen et du Conseil du 9 mars 1999, concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, *J.O.C.E.*, n° L 091 du 7 avril 1999, pp. 10-28, EUR-*Lex*, http://eur-lex.europa.eu.

Cette définition très large permet d'englober non seulement les ordinateurs personnels, les terminaux classiques comme le téléphone (mobile ou non), le fax ou autres mais également les RFID [48], les cartes à puces [49] et demain, les molécules « intelligentes » implantées au sein même du corps des individus.

Ce qui caractérise les RFID dont le marché se développe à une allure exponentielle [50] est tant leur miniaturisation, que le fait qu'ils s'attachent et identifient la possession d'un objet même si indirectement les informations ainsi générées révèlent le comportement du possesseur de l'objet. Ce fait soulève la question de savoir si nos législations relatives à la protection des données « identifiant » des personnes sont applicables [51], lorsqu'il s'agit d'identifier un objet.

48. Ces terminaux que sont les RFID possèdent les éléments suivants :
    - un processeur ;
    - une mémoire morte ;
    - une antenne qui permet tout à la fois de communiquer avec un terminal et de recevoir l'énergie requise pour faire fonctionner l'ordinateur ;
    - absence de périphériques d'entrée/sortie accessibles à un être humain ;
    - très haut degré de miniaturisation (de l'ordre de quelques millimètres, antenne incluse) Sur les RFID, le lecteur consultera le site très complet : http://www.rfida.com/nb/identity.htm.
49. Certaines cartes à puces sont équipées de processeurs aussi puissants que les célèbres Apple du début des années 80.
50. Le marché des RFID's se déploie à une échelle mondiale pour identifier et tracer la plupart des biens matériels. On a cité comme cas les chemises Benetton ou les rasoirs Gillette. Les arguments généralement avancés sont la lutte contre le vol en magasin et un environnement ambiant plus intelligent qui permettraient aux objets même les plus insignifiants de communiquer avec leur utilisateur. Une autre utilisation possible est constituée par le numéro de série qui pourrait être gravé dans cette puce scellée dans l'objet.
    Le système de codification des RFID est révélateur de son ambition. Le code EAN (European Article Number) se compose de 96 bits dont les 36 derniers sont réservés pour le seul numéro de série de l'article. Il s'agit donc de permettre l'identification individuelle de 16 milliards d'objets identiques (du même type et produits par la même firme). Si on ne voit pas quelle entreprise pourrait produire 16 milliards de produits identiques ni l'utilité de différencier le cas échéant ces milliards d'objets identiques, on notera qu'il s'agit de l'ordre de grandeur de la taille prévisible de la population mondiale dans les décennies à venir.
51. Nous reviendrons sur ce point *infra*, n° 33. On note que la proposition de directive (COM (2007) 698 final, EUR-*Lex*, http://eur-lex.europa.eu, qui a fait l'objet d'un avis 2/2008 du Groupe de travail de l'article 29, WP150 : http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_fr.htm) modifiant la directive 2002/58/CE entre autres par un changement qualifiée de « technique » à l'article 3.1. Cette modification vise à préciser que la directive s'applique aux réseaux de communications publiques qui prennent en charge le dispositif de collecte de données et d'identification, en ce compris les dispositifs sans contacts, tels que des systèmes d'identification par radio fréquence. On observe donc que pour la Commission, en cohérence avec son projet de recommandation, la directive 2002/58 régit bien partiellement les RFID, mais que, ce qui va sans dire, va encore mieux en l'écrivant...

Au-delà de ce premier phénomène, on souligne deux autres points majeurs relatifs à l'évolution des terminaux. Ainsi, premier point, en ce qui concerne la nature de l'équipement terminal, la technologie est passée de l'électromécanique à une électronique programmable. En d'autres termes, le fonctionnement de l'équipement terminal est dicté par un déterminisme qui est celui non de l'utilisateur [52] mais du concepteur de l'appareil, voire de tiers qui peuvent insérer dans le terminal des applicatifs permettant une utilisation à distance de ce terminal (ainsi les *spywares* ou l'ensemble des logiciels de mise à jour de programmes installés sur l'ordinateur) [53]. Bref, l'utilisateur d'un terminal n'a qu'une maîtrise partielle de l'ordinateur, sans que l'utilisateur ne soit à l'initiative de ces flux.

Cette absence de maîtrise par l'utilisateur se double d'une perte totale par l'État de tout contrôle des normes de production des équipements terminaux.

Là où le fonctionnement du terminal téléphonique « classique » était sévèrement réglementé, ce n'est plus le cas en ce qui concerne les normes techniques et fonctionnelles qui président au développement de la micro-informatique [54].

19. La multifonctionnalité des terminaux et la convergence des réseaux

Une seconde caractéristique est la « multifonctionnalité » présente dans la plupart des équipements terminaux (micro-ordinateurs mais également les nouvelles générations de GSM). La traditionnelle répartition des médias en fonction de leur capacité fonctionnelle (téléphone = transport de la voix ; télévision = transport de l'image et du son...) disparaît grâce à la numérisation de tout contenu [55] au profit d'une convergence qui permet à un terminal

52. À propos de la parfaite transparence et maîtrise du fonctionnement des anciens terminaux comme le téléphone ou le fax, lire Y. POULLET et J-M. DINANT, « L'autodétermination informationnelle à l'ère de l'Internet », Rapport pour le Conseil de l'Europe, novembre 2004, déjà cité.

53. Sur le fonctionnement de ces logiciels intrusifs, lire http://www.clubic.com/actualite-21463-phishing-et-spyware-les-menaces-pesantes-de-2005.html.

54. Les organes de normalisation et de standardisation en matière de technologie de l'information et de la communication sont de plus en plus des organes privés échappant au contrôle des organisations publiques. Sur les débats du Sommet Mondial de la Société de l'Information qui maintient le caractère privé de l'ICANN qui régule les ressources rares de l'Internet, lire les documents publiés par la « Markle Foundation » dont le « Guide to International ICT Policy Making » publié en 2003 et accessible sur le site de la Fondation. Et de manière générale sur ce phénomène, lire la thèse de Ph. AMBLARD, *Régulation de l'Internet : L'élaboration des règles de conduite par le dialogue internormatif*, Cahier du CRID, n° 22, Bruylant, Bruxelles, 2005.

55. Ainsi, les normes : JPEG pour les photos ; EFR pour la voix ; MPEG pour les images en mouvements, permettent la normalisation de tout signal audio ou images.

de fonctionner pour de multiples usages et dès lors, autorise certains acteurs comme les fournisseurs d'accès ou toute personne intervenant dans le routage, voire dans l'aide à la sélection des sites, de croiser désormais des données nées de l'utilisation de ces diverses fonctionnalités (ainsi, le téléphone, l'écoute de programmes radio, l'envoi de correspondance, le suivi de programmes de télévision...).

2. *L'évolution de l'Internet*

20. Convergence des réseaux et globalité

La révolution de l'Internet à laquelle nous continuons d'assister présente des dimensions diverses. Il est de coutume d'insister sur la globalisation des échanges qui me permet, sans bouger de l'endroit où je me trouve, d'atteindre les quatre coins du monde. L'on parle également, invoquant les modèles de quatrième génération des télévisions interactives, de la convergence de tous les réseaux, là où nos activités de communication étaient jusque là séparées, véhiculées par des infrastructures différentes.

21. Web sémantique

Notre propos ne s'arrête pas là. Afin de mieux inter-opérer, de dialoguer entre eux, de pouvoir comprendre les messages transmis, le web est devenu sémantique [56], ce qui veut dire que l'ordinateur lui-même crée des métadonnées à partir de données qu'il stocke ou envoie de manière à ce que, plus facilement, les personnes, voire les ordinateurs, puissent à distance accéder et analyser leur contenu. Les services d'analyse automatique des courriers électroniques sont un bel exemple de cette dimension nouvelle. Grâce à cette intelligence nouvelle, les systèmes d'information sont capables d'analyser le contenu de bases de données sans qu'aucune structure prédéfinie ne soit nécessaire. Nous ne saurions trop insister sur le fait que cette création de métadonnées, qui permet de découvrir l'information à travers le filtre de mots-clés et de la conceptualisation inhérente au web sémantique, n'est plus nécessairement ni volontaire ni consciente dans le chef de celui que l'on nomme l'« utilisateur », mais bien plutôt le résultat d'opérations automatiques réalisées par l'ordinateur.

22. Web 2.0

Le web 2.0 regroupe des pratiques caractérisées par une participation active des utilisateurs à la création et au fonctionnement de sites en ligne. Il s'agit

56. Sur cette évolution du fonctionnement du Web lire M. RUNDLE, *Ethical implications of emerging technologies in the Information Society*, UNESCO Publications, 2006.

tantôt des réseaux dits sociaux, des encyclopédies du type Wikipedia ou des sites de partage de contenus comme *You Tube* ou *Dailymotion*. Ces pratiques soulèvent des questions nouvelles en matière de protection des données à caractère personnel [57]. Tout d'abord, parce que ces pratiques concernent des données parfois intimes fournies activement et volontairement par les internautes : des émotions, des réseaux d'amis, des faits de leur vie ou de tiers, un état de santé ; ensuite parce que ces données sont relatives à eux-mêmes ou à des tiers.

Ainsi, l'internaute peut jouer à la fois les rôles traditionnellement distingués, celui de personnes concernées et celui de responsables de traitement.

Les applications présentes dans ces pratiques permettent au fournisseur du service mais également à des tiers de les profiler en fonction des contenus mis à disposition et des données d'utilisation du site [58] et surtout d'utiliser de telles données « hors contexte », ainsi, lorsque l'employeur analyse les communications opérées, le réseau d'amis, les échanges effectués et les données mises par un candidat employé dans le contexte d'un réseau social [59]. On note que le réseau conserve la mémoire d'événements qui n'avaient, pour celui qui les a placés, de sens que très temporaire. Enfin, on s'inquiète de la façon dont espace privé et espace public s'entremêlent à l'occasion des relations nouées dans ces contextes.

23. Les méthodes d'identification et d'authentification - *digital identities* : pourquoi ?

Une autre évolution remarquable de l'Internet résulte de la disponibilité et de l'utilisation de méthodes d'identification et d'authentification des acteurs/utilisateurs du net. Ces méthodes permettent à ces derniers à la fois de se faire connaître ou reconnaître lorsque cette « identification » conditionne l'accès à une ressource (*cf.* les systèmes dits *d'Identity Management*), un service ou une

57. Pour de plus amples réflexions, lire G. GONZALES FUSTER et S. GUTWIRTH, « Privacy 2.0 ? », *R.D.T.I.*, 2008, n° spécial Web 2.0, pp. 351-379, http://www.strada.be ; *cf.* également le rapport et les recommandations de l'International Working Group on data Protection in Telecommunications : *Report and Guidance on Privacy in Socal Network Services,'Rome Memorandum'*, 43e réunion, Roma, March 2008.

58. Sur ces diverses « agrégations de dossiers » et leur réel danger pour la vie privée, lire le rapport HOGBEN (ed.), *Security Issues and Recommendations for Online Social Networks*, ENISA, Position Paper n° 1 ; Heraklion, Grèce, octobre 2007, pp. 3 et s.

59. Cette « décontextualisation » est d'autant plus importante que les réseaux ne sont pas thématiques et mêlent des relations tant professionnelles que privées d'ordre divers (ainsi lorsqu'un usager fait partie à la fois d'un réseau d'anciens de collège, d'un club de footballeurs, d'un réseau de fans de Madonna, etc.).

information et, au-delà, de pouvoir les identifier de manière sûre lorsqu'il s'agit d'additionner, de croiser, voire de déduire des données nouvelles à leur propos et ce, à partir d'éléments d'information dispersés dans des bases de données distribuées dans le réseau et ce, sans limites de frontières [60]. On note que ces *digital identities* constituent alors des métadonnées qui permettent de croiser les informations relatives à une personne dans des bases de données diverses [61]. On souligne le danger lié à l'utilisation de *digital identities* communes à plusieurs secteurs de notre existence. Il est évident que plus une méthode d'identification est commune à de nombreuses bases de données, plus le croisement de ces bases de données est facile. Ainsi, dans le secteur public, on sait que la généralisation du numéro de registre national à l'ensemble des bases de données de l'administration accroît le risque de croisement de ces bases de données et donc le pouvoir de l'administration vis-à-vis du citoyen. De manière générale, c'est toute la question de l'intégrité contextuelle, le fait que des données collectées dans des « contextes » différents soient regroupées, qui se trouve posé par ce partage d'identifiants entre responsables de traitement. Nous reviendrons sur ce point (*infra*, n° 35).

24. Les méthodes d'identification et d'authentification - *digital identities* : comment ?

Enfin, soulignons l'évolution de nature de ces identités digitales. Si les premières « identités » étaient liées à des données dont la teneur était directement identifiante, comme le nom et ou l'adresse, avec les numéros de GSM, les mots de passe et les signatures électroniques, on passe à des identités non directement identifiantes mais qui reposent sur une donnée connue de l'individu. Les *cookies*, les numéros inscrits dans les tags RFID ne sont plus nécessairement connus de l'individu mais liés à la possession d'un objet dont la numérotation est le fait d'un tiers et dont l'attribution est maîtrisée par celui-ci ou par les entreprises qui les placent. Avec les technologies de la biométrie (l'iris,

60. C'est ce que nous avons appelé les données d'ancrage, données à caractère personnel qui permettent de faire le lien entre des données relatives à un même individu mais localisées dans des bases de données diverses. Cette notion s'oppose aux données biographiques qui décrivent un élément de la vie de l'individu ou le caractérisent. Notre propos était de souligner l'insuffisante attention portée par les législations de protection des données à cette catégorie de données. Y. POULLET et J.-M. DINANT, « L'autodétermination informationnelle à l'ère de l'Internet », Rapport pour le Conseil de l'Europe, novembre 2004, déjà cité.

61. Sur ces dangers, M.C. RUNDLE et P.TREVITHICK, « Interoperability in the new Digital Identity Infrastructure », *(Feb. 13, 2007)* papier publié sur Social Science Research Network, disponible sur le site : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=962701 ; M.C. RUNDLE, « International Personal Data and Digital Identity Management Tools », Research Publication Paper, *The Berckman Center for Internet and Society*, n° 2006, June 2006, disponible sur site : http://cyberlaw.law.harcvard.edu/publications.

l'empreinte des doigts, la voix), l'identité et l'identifiabilité « s'incarnent » dans des caractéristiques physiques et corporelles, réduites à leurs représentations en données. Ici également on note une évolution puisque la donnée biométrique peut concerner une caractéristique physique extérieure de l'individu comme dans les exemples précédents ou s'inscrire plus profondément dans la génétique de l'individu. Quoi qu'il en soit, ces données génétiques présentent une particularité celle de suivre l'individu jusqu'à sa mort.

À l'inverse des autres données d'identification et d'identifiabilité, elles ne sont pas prescriptibles ni effaçables par la volonté de celui qu'elles identifient [62].

3. *L'intelligence ambiante : où le virtuel rejoint le réel*

25. Le lien entre virtuel et réel : de la géo localisation aux RFID

Sans doute faut-il à propos du lien possible permis par les technologies entre virtuel et réel évoquer, en premier lieu, les nombreux services de localisation spatiale qui offrent une aide au destinataire spécifique au lieu où il se trouve (services de navigation, mais également services relatifs aux caractéristiques de l'environnement proposés en lien avec la possession d'un mobilophone).

Les réseaux d'intelligence ambiante permettent d'autres applications liant le monde réel et celui virtuel. Ils ont pour objet de mettre la personne et son environnement directement en interaction. L'intelligence que permettent les T.I.C. et l'accès au cyberespace est dorénavant répartie dans les choses, les lieux, voire nos corps, dans lesquels, selon la vision prophétique de l'ingénieur Weiser [63], la technologie se fond pour devenir une seconde nature. Ces technologies de l'intelligence ambiante doivent leur développement à l'extrême miniaturisation des terminaux (*cf.* les RFID et les nanotechnologies encore dans l'enfance de la recherche et leur connexion via des capteurs et l'Internet à des systèmes d'information). Les applications sont multiples et permettent, par exemple, de suivre le parcours d'un consommateur dans un supermarché et, grâce au « dialogue » entre la puce du consommateur et celles des produits, de comptabiliser automatiquement les achats effectués. Elles peuvent aussi permettre de lire, à distance, des passeports, « faire commander » automatiquement, par un « frigo intelligent », la bière manquante, ou encore faire en sorte

62. Sur cette évolution lire D. DARQUENNES et F. DUMORTIER, « L'utilisation de la biométrie et de la technologie RFID dans le cadre de l'espace européen de liberté, de sécurité et de justice : une question de balance ou de dignité ? », Actes du colloque organisé par l'ERA, Sécurité et vie privée, mars 2008, à paraître dans la série ERA FORUM, Vol. 10, Springer Verlag, 2008.

63. M. WEISER, « The computer for the 21st Century », *Scientific American*, 1991, Vol. 265, n° 3, pp. 66–75.

qu'un poste de télévision repère automatiquement votre présence et envoie l'image du programme adéquat automatiquement vers l'écran de l'ordinateur personnel de votre bureau. Les applications sont infinies. Elles permettent de caractériser l'intelligence ambiante comme suit.

26. L'*Ubiquitous computing*

On parle de technologie de l'ubiquité (*ubiquitous computing*) dans la mesure où les terminaux peuvent être placés partout et dès lors enregistrer les faits les plus anodins de notre vie quotidienne, nos déplacements, nos hésitations, notre consommation domestique. Cette technologie est ensuite une technologie largement invisible (*calm technology*) dans un double sens : elle fonctionne de manière opaque, invisible (nous ne connaissons pas le circuit d'information sous-tendant le fonctionnement de la puce : qui la lit ? Quand ? Quelles informations ? Pour qui ?), mais également elle apparaît comme le prolongement naturel même de notre action (la porte s'ouvre et l'ordinateur s'allume) mettant les choses à notre service. Enfin, cette technologie est dite « apprenante » (*learning technology*). Ses applications ont souvent en effet pour caractéristique d'adapter leur fonctionnement aux données obtenues de par leur utilisation. Ainsi, dans le cas du grand magasin, le système tiendra compte de nos achats précédents pour progressivement mieux nous profiler et nous adresser la publicité la plus appropriée.

Ainsi, les technologies d'intelligence ambiante ont pour conséquence d'associer le virtuel et le réel. Au sein des réseaux créés par le dialogue entre les choses entre elles ou avec l'homme, c'est l'espace réel qui se trouve investi par les technologies de l'information et de la communication [64]. Au sein de ces réseaux, l'homme, *in fine*, peut devenir une « chose » elle-même insérée dans une relation avec d'autres choses qui réagissent à la présence de cette chose.

On évoquera enfin les questions liées aux applications dites « médicales » des RFID implantés dans le corps humain qui permettent à distance de connaître le fonctionnement de celui-ci, voire de « corriger » ce fonctionnement, par exemple remédier à un état de stress ou stimuler la mémoire.

27. Les raisons du succès des technologies d'intelligence ambiante

Cinquante pour cent des habitués des *Baya Club* [65], une société de gestion de dancings et maisons de jeux situés en Hollande et Espagne, ont accepté de se voir implanter une puce RFID dans le corps. Aux journalistes qui s'inquiétaient

64. Sur cette question, lire A. ROUVROY, « Privacy, Data Protection, and the Unprecedented Challenges of Ambient Intelligence », *Studies in Ethics, Law, and Technology*, Berkeley Electronic Press, 2008.

65. *Cf.* le célèbre cas de la discothèque *Baja Beach Club* implantée aux Pays-Bas et en Espagne (http://www.baja.nl).

de leur acceptation, ceux-ci répondent qu'une telle puce facilite grandement leur passage aux entrées du casino où la lecture de la puce permet de les reconnaître comme « bons » clients et, par ailleurs, leur permet de ne pas courir le risque de se voir voler leur portefeuille, inutile dans la mesure où les consommations leur sont directement débitées de leur carte de crédit. Cet exemple – et on pourrait les multiplier – illustre combien les logiques sécuritaires et d'efficacité économique (gain de temps, voire d'argent) expliquent le succès des applications. C'est la puce RFID que le gouvernement américain entendait implanter dans le corps de tout citoyen américain pour qu'en cas d'accident et en suite d'inconscience de ce dernier, on puisse l'identifier et connaître les données médicales d'urgence. Dans le même ordre d'idées, on rappelle l'émotion créée en Belgique par la découverte de l'implantation d'une puce RFID dans les passeports, implantation « à des fins de sécurité » et la forte réticence y compris des fabricants de microprocesseurs par rapport à la même initiative prise par l'administration américaine [66].

Ainsi, la sécurité, celle publique mais également celle privée des organisations et des citoyens, exige toujours plus la mise sur pied de systèmes de contrôle, de surveillance et d'alerte [67]. La rentabilité économique, au sens le plus large, l'efficacité tout court, viennent comme une justification complémentaire où se rejoignent les préoccupations des administrations et des organisations, d'une part, et les intérêts des consommateurs et des citoyens, intérêts soigneusement mis en évidence par les administrations ou organisations, d'autre part.

B. Deux tendances majeures

1. *La privatisation du cyberespace*

28. Les significations de la notion

Sous ce point, on souligne le fait que les normes applicables dans le cyberespace et le fonctionnement du réseau (adresses IP, protocoles web...) échappent en

66. À cet égard, les conclusions de la Smart Card Alliance du 3 novembre 2006 (disponible sur le site : http://www.smartcardalliance.org/pages/publications-whti-passport-card) à propos de l'utilisation de la technologie RFID dans les passeports et la possibilité de lire à distance ceux-ci : « La lecture de proximité des puces nées de la technologie RFID proposées pour le passeport, en combinaison avec la faiblesse de protection cryptographique, viendra nourrir la méfiance des citoyens en raison de l'observation indéniable par certaines technologies que le numéro unique de référence des citoyens pourraient être obtenus et utilisés pour suivre le citoyen lorsque la carte est à l'extérieur de sa gaine protectrice. Cela soulève de graves problèmes de confidentialité qui doivent être surmontés si le programme doit être adopté par les américains » (traduction libre). Dans le même sens, la Déclaration de Budapest sur les documents de voyage à lecture automatique (MRTD-Machine Readable Travel Documents) disponible sur le site de la FIDIS (projet de recherche européen) : http://www.fidis.net/press-events/press-releases/declaration-de-budapest.

67. À ce propos, D. LYON, « Surveillance Society, Understanding Visibility, Mobility and the Phenetic Fix », in *Surveillance and society*, Vol.1 (1), pp. 1 et s., 2002.

grande partie aux autorités publiques qu'elles soient nationales, régionales ou internationales. La gouvernance de l'Internet est privée.

Elle est l'œuvre au premier chef d'organisations privées internationales comme le W3C, l'IETF et l'ICANN [68] et, en tout cas, résulte de la discussion de sociétés privées plus que d'arbitrages interétatiques.

La privatisation du cyberespace prend une autre signification lorsqu'on doit bien constater que l'accès à ce cyberespace, tant pour les destinataires que ceux qui veulent y mettre du contenu, se trouve conditionné au respect des exigences imposées par certains acteurs, les fournisseurs d'accès, les portails, les moteurs de recherche qui peuvent orienter notre recherche de l'information, notre navigation et la soumettre à l'acceptation par nous de règles du jeu, telles la publicité, l'identification, etc. [69] C'est souvent eux aussi qui apposeront des filtres, des limites, voire des procédures de censures et s'auto-constitueront ainsi, tacitement, en régulateurs de l'espace public qu'est l'Internet.

Toujours dans le même sens, on connaît la contestation que soulèvent certains *Digital Rights Management Systems* (D.R.M.S. ou systèmes de gestions des droits numériques) [70] lorsque la technique, bien au-delà des principes et de la logique des droits de propriété intellectuelle, clôture l'œuvre et en restreint excessivement l'accès, au détriment de l'exercice, par d'autres, de leurs libertés fondamentales ou de l'accès par tous à certaines œuvres essentielles.

Enfin, on note que les technologies de surveillance dont les applications se multiplient dans les espaces ouverts au public (galeries commerciales, grandes surfaces, discothèques et autres) entraînent une privatisation d'un espace jusqu'alors d'anonymat et entraînent, outre des pratiques de surveillance de

68. Sur l'importance de ces organes de normalisation privés, lire P. TRUDEL *et alii*, *Droit du cyberespace*, Montréal, Themis, 1997, Livre 3 et la critique de cette privatisation par M.A. FROOMKIN, « Habermas@discourse.net : Towards a critical theory of Cyberspace, 116 *Harvard Law Rev.*,1996, pp. 800 et s.

69. Ce qui est encore plus inquiétant si l'on sait que 49 % des internautes accèdent à l'Internet via un moteur de recherche (selon une analyse du cabinet d'études Pew Internet et American Life Project rapportée par le New York Times – http://www.clubic.com/actualite-155336-les-moteurs-de-recherche-en-pleine-croissance.html) et qu'en plus un moteur comme *Google* peut être affecté de bugs tels celui qui l'a amené pendant une heure à dire le 31 janvier 2009 aux internautes que tout site pourrait endommager leur ordinateur et partant, à réduire durant cette période 21 % du trafic sur l'Internet.
À propos des D.R.M. et des questions de vie privée soulevées par ces systèmes de réservation d'œuvre, lire notamment L. BYGRAEVE, « Digital Rights Management and Privacy : Legal Aspects in the European Union », *in* E. Becker *et al.*, *Digital Rights Management : Technological, Economic, Legal and Political Aspects* (Heidelberg : Springer Verlag, 2003), pp. 418–446.

nos gestes et actions, l'exclusion de certains groupes sociaux comme en témoignent des études sociologiques [71].

2. *La portée globale d'actions ou de décisions d'acteurs locaux*

29. La société de l'information et sa réglementation : un parallèle avec la réglementation de l'environnement [72]

Parmi les acteurs locaux, on épinglera bien évidemment les entreprises qui offrent des services grâce à ces technologies. La façon dont leurs produits ou services sont construits peut avoir des répercussions sur l'ensemble de la planète lorsque la puissance économique que ces entreprises détiennent est telle qu'elle leur permet de décider des conditions d'accès à l'information ou de publication de contenus d'une partie de la population mondiale. Il faut bien se rendre compte notamment que l'Internet décuple la puissance de certaines entreprises de presse.

Mais l'Internet décuple également la puissance de l'individu lui-même qui, de manière ciblée ou diffuse, consciemment ou inconsciemment, peut, par un simple message posté sur le net, une simple information sur son blog, porter atteinte à la réputation d'autrui, transmettre un virus, envoyer ou consommer des contenus pédopornographiques et, de ce fait, encourager la traite des êtres humains, autant d'actes faciles à poser localement qui peuvent avoir des répercussions dommageables jusqu'à l'autre bout de la planète. Internet confère donc à nos actes, même individuels, et sans aucun effort particulier de notre part, une portée « globale » qui n'est pas sans reposer la question de la responsabilité individuelle et collective.

Il nous paraît peut-être fécond, à cet égard, de penser en terme d'écosystème informationnel, de la même façon que les défis actuels posés par la dégradation de l'environnement naturel nous ont induit à penser nos responsabilités individuelles en termes plus globaux. Sans doute, une autre dimension des relations humaines, de plus en plus cernée par les technologies de l'information et de la communication, celle de l'espace, inviterait donc à s'inspirer des principes d'une éthique de l'environnement. Les principes du développement durable, et surtout ceux du risque partagé et de précaution

71. A. WAKEFIELD, « The public surveillance Functions of Private Security », *Surveillance and Society*, 2005, 2 (4).

72. Y. POULLET et A. ROUVROY, « Le droit à l'autodétermination informationnelle et la valeur du développement personnel – Une réévaluation de l'importance de la vie privée pour la démocratie », *in État de droit et virtualité, Actes du colloque organisé à Montréal par la Chaire L.J. Wilson*, octobre 2007, à paraître.

mis en évidence dans cet autre domaine mais qui n'ont pas encore fait l'objet du même consensus que celui qui s'est dégagé dans le domaine de la bioéthique, pourraient également nous être utiles.

SECTION 3
De quelques pistes et conseils pour assurer une protection des données dans notre société de l'information

30. Où il est question des limites mais également de l'intérêt des concepts essentiels de nos législations relatives aux données à caractère personnel

Nos législations sont-elles à la hauteur des défis que notre société de l'information soulève ? Notre propos sur ce point est double. D'une part, il est clair que le développement des applications décrites dans le titre I oblige à s'interroger sur les insuffisances de l'approche législative jusqu'ici tenue. Si les législations de protection des données à caractère personnel s'inscrivent comme une réponse adéquate aux risques que courraient nos libertés en 1995, soit avant l'ère de l'internet de la convergence et de l'intelligence ambiante, cette adéquation n'est plus aujourd'hui réalisée. À cet égard, l'analyse de certaines dispositions de la directive 2002/58/C.E., dite directive *e-privacy*, révèle les germes d'une nouvelle génération de législations de protection des données ! Le plan de la section III est la suivent : nos législations de protection des données législations vie privée, que nous qualifierons de troisième génération (A). Par ailleurs, même si cette troisième génération est nécessaire, il est évident qu'elle doit s'appuyer sur les principes de proportionnalité et de transparence qui sont au cœur des législations de deuxième génération celles actuellement en vigueur dans nos pays (B).

A. Vers une troisième génération de législations de protection de la vie privée [73]

31. De la protection conférée par l'article 8 CEDH et la Directive 95/46

L'histoire de la protection des données prend naissance avec l'article 8 de la Convention européenne des droits de l'homme [74]. La disposition laisse

73. Nous avons développé cette idée de troisième génération dans l'article « Pour une troisième génération de réglementations de protection des données », *in dans Privacy- New visions*, M.V. Perez et A. Palazzi (eds), Cahier du Crid, 2008, pp. 25-70.

74. *Supra* n° 4.

concevoir la vie privée comme le « droit d'être laissé seul » [75], lié au droit à l'intimité des personnes. Celui de ne pas voir révéler des informations liées à sa « sphère privée », qu'elle soit physique, le domicile familial, ou qu'elle soit l'expression d'une relation à autrui, le secret de la correspondance [76]. La vie privée apparaît ainsi au départ comme un concept indéfini qui ne peut s'approcher que de manière négative et souple. Il s'agit d'informations « sensibles » certes mais au-delà, d'abord de lieux (le domicile) et de relations d'un type particulier (l'espace familial et la correspondance) dont la révélation à des tiers ou la mise sur la scène publique priveraient l'individu de l'espace suffisant pour pouvoir exprimer et forger sa propre personnalité et exercer ses libertés fondamentales [77].

La première génération de protection de la vie privée, essentiellement caractérisée par une approche fondée sur la nature de la donnée, était-elle sensible ? Appartenait-elle à la sphère intime de la personne concernée ? L'autodétermination informationnelle est alors comprise comme l'interdiction de traiter certaines données et la protection de certaines sphères tant physiques que communicationnelles.

La deuxième génération [78] ajoute à la première la nécessité, au-delà de la protection de ces données particulières, d'envisager la façon dont le traitement de données à caractère personnel peut modifier les relations de pouvoir entre celui qui traite les données et celui à propos duquel le traitement a lieu. L'« autodétermination informationnelle » suppose la nécessité de rééquilibrer la relation en garantissant la transparence des traitements et en limitant le droit de traiter les données d'autrui. Cette deuxième génération qui englobe la directive dite générale de protection des données de même que l'article 8 de la Charte européenne des droits de l' Homme qui en est le prolongement semble aujourd'hui insuffisante à prendre en compte les risques encourus par les libertés des citoyens du fait des technologies de l'information et de la communication. On rappelle que la directive de 1995 n'a pu prendre en compte le fait de l'Internet et des nouveaux réseaux numériques, ni d'ailleurs la directive 97/66/C.E. dite RNIS et vie privée. La prise en considération de ces nouveaux réseaux et des utilisations dont on perçoit seulement aujourd'hui les premiers développements amène à devoir considérer un élargissement de la protection des données au-delà des principes mis en place par la directive 95/46/C.E. Si la technologie de l'information et de la communication est prise en compte en 1995, son impact est perçu du seul côté du responsable comme un accroissement de leurs pouvoirs et crée dès lors des obligations à la charge de ces derniers de veiller à la sécurité technique et organisationnelle des traitements, la notion de sécurité étant entendue au sens le plus large.

75. Le fameux *Right to be left alone* défendu par S. WARREN et L. BRANDEIS dans leur article : « The right to privacy », 4, *Harvard Law Rev.*, 193 (1890), http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html.

76. À ce propos, la Recommandation 428 (1970) du Comité d'experts du Conseil de l'Europe portant déclaration sur les moyens de communication de masse et les droits de l'homme, Annales de la Conv. Vol. 13, 1970, p. 65.
Ainsi, P. DE HERT et S. GUTWIRTH (« Privacy, Data Protection and Law Enforcement, Opacity of the individuals and Transparency of power », *Privacy and Criminal Law*, (E. CLAES, A. DUFF and S. GUTWIRTH (ed.)), Intersentia, Antwerpen-Oxford, 2006, pp. 61et s.) parlent de « droit à l'opacité » (*Right to opacity*) par opposition au « droit à la participation » qui caractérise la seconde génération de réglementation « vie privée ». À noter, leur plaidoyer fondé pour un retour de ce droit à l'opacité dans nos sociétés modernes dites de l'information.

78. *Supra* n[os] 9 et 12.

La révolution que représentent les réseaux numériques pour la protection des données repose sur le fait qu'entre le responsable du traitement tel que conçu par la directive et la personne concernée, la technologie s'interpose à un double titre. Comme nous l'avons montré, elle est à la base de flux conscients ou inconscients provenant du terminal de la personne concernée ou d'un objet qui autorise le contact avec cette personne, même non identifiée voire non identifiable. Par ailleurs, le réseau lui-même ne constitue plus, comme c'était le cas dans la communication par circuits, un lien unique entre un émetteur et un destinataire, mais autorise un foisonnement de relations non contrôlées où interviennent, à partir de lieux multiples et sans considération de frontières, des intervenants connus ou inconnus.

Bref, c'est cette technologie dont la présence et les caractéristiques forment l'interface entre la personne concernée et ces intervenants qu'il importe désormais de réglementer. À notre opinion, la directive 2002/58/C.E. contient les éléments de base de cette nouvelle approche.

32. ... à la directive européenne 2002/58 comme amorce d'une troisième génération de protection

Traditionnellement, la directive de 2002 est considérée comme une application ou spécification [79] des règles contenues dans la directive de 1995 dite directive générale. Elle constitue une révision de la directive sectorielle 97/66/C.E. du 15 décembre 1997 concernant le traitement de données à caractère personnel

9. À cet égard, lire S. LOUVEAUX et M.V. PEREZ-ASINARI, « *New European Directive 2002/58 on the processing of personal data and the Protection of Privacy in the Electronic Communications Sector* », (2003) CTLR, 5, p. 133 ; W. MAXWELL (ed.), « *Electronic Communications : The new EU Framework : Booklet I.5 : The Communications Data Protection Directive* », Oceana, Dobbs Ferry, New York, 2002.

et la protection de la vie privée dans le secteur des télécommunications [80] et l'adaptation de cette dernière à l'évolution du marché des technologies et des services de communication et aux risques nouveaux liés à cette évolution.

Notre propos est de suggérer une autre lecture : l'adoption de la directive de 2002 en cours de révision [81] marque, sur certains points limités, certes, mais importants, une rupture avec la conception traditionnelle de la protection de la vie privée, consacrée par la directive 95/46/C.E [82]. Notre thèse s'appuie sur le fait qu'à la fois en ce qui concerne les données protégées, les personnes soumises à des obligations et les objets réglementés, la directive de 2002 déborde le champ d'application de celle de 1995.

33. Des données protégées au-delà des données à caractère personnel

La définition même des « données », dont la protection est au cœur même de la directive de 2002 ne suit pas exactement celle de 1995. Les définitions de « données de trafic » et de « localisation » reprises à l'article 2 évitent soigneusement les expressions de « données à caractère personnel », qui circonscrivent pourtant le champ d'application de la directive 95/46/C.E., dont la directive de 2002 ne serait qu'une application. Autant l'article 2 c) que le considérant 14 de la directive définit la donnée de localisation par la seule référence à l'équipement terminal d'un utilisateur. Lorsqu'il s'agit de commenter la notion de donnée de trafic, le considérant 15 parle « d'informations consistant en une dénomination, un nombre ou une adresse, fournie par celui qui émet la communication ou celui qui utilise une connexion pour effectuer la communication ». On ajoute que la directive protège également la personne morale, ce qui va au-delà de la directive de 1995.

Qu'est-ce à dire ? Ces données peuvent ne pas être des données à caractère personnel, en d'autres termes que la recherche du lien avec une personne identifiée ou identifiable n'est plus nécessaire. Le pas est clairement franchi par un avis du Groupe dit de l'article 29 à propos de la notion de données à caractère personnel [83] lorsqu'il propose de définir la notion de donnée à caractère personnel non plus en fonction de l'« identifiabilité » de la personne concernée comme le requiert strictement le prescrit de l'article 1er de la

80. Directive 97/66/C.E. relative aux traitements de données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, *J.O.C.E.*, L024/1, 24 janvier 1998; EUR-*Lex*, http://eur-lex.europa.eu.

81. Sur la révision actuellement en cours, voir *supra* note 13.

82. À ce propos, l'article 1.2. de la directive 2002/58 note à juste titre : « Les dispositions de la présente Directive précisent et complètent la directive 95/46/C.E. ... »

83. Avis 4/2007 sur le concept de données à caractère personnel, 20 juin 2007, W.P. 136.

directive, mais en fonction de l'impact que, grâce à certaines données, en particulier celles qui permettent d'assurer le contact avec un terminal (par exemple les *cookies* ou les objets munis d'un RFID), une personne peut avoir par rapport à une personne. Ainsi, si je munis le caddie d'un visiteur de supermarché d'un RFID qui me permet de localiser l'emplacement de celui-ci dans le magasin et de connaître les achats effectués par celui-ci, le supermarché peut envoyer sur une vidéo placée sur le caddie la publicité adéquate, sans que celui-ci ne soit pour autant identifié.

Sans doute, dira-t-on, l'article 3 à propos des « services concernés » par la directive n'évoque que les « traitements de données à caractère personnel dans le cadre de la fourniture de services de communications dans la Communauté ». Dans la mesure où d'autres dispositions de la directive, comme il sera montré plus loin, réglementent des situations qui excèdent le champ d'application de l'article 3, on n'y prêtera pas nécessairement attention. Il suffit en effet, selon la définition de la donnée de trafic ou de localisation, qu'un lien puisse être fait avec un terminal, un objet et qu'à travers celui-ci une personne, le possesseur de ce terminal même non identifié puisse soit être atteint, soit être caractérisé pour que cette directive nouvelle s'applique. Une telle conception permettrait demain de réglementer les systèmes d'intelligence ambiante, fondés sur la technologie dite RFID, qui entendent manipuler des données relatives à un objet pour prendre des décisions vis-à-vis de leurs possesseurs sans s'intéresser à « identifier », au sens classique du terme [84], ces derniers. En d'autres termes c'est la possibilité, grâce à des données, de prendre des décisions vis à vis de certains individus identifiés ou non, identifiables ou non, qui doit être entourée de garanties.

C'est, nous semble-t-il, la direction que prend la Commission lorsqu'elle suggère dans son projet de recommandation des obligations détaillées, alors même qu'« une application RFID n'implique pas le traitement de données à caractère personnel et lorsque l'évaluation d'impact sur la vie privée a mis en évidence un risque négligeable que des données à caractère personnel soient produites

84. Cette question est largement débattue dans l'opinion du groupe dit de l'article 29 dans le Working document on Data Protection Issues to RFID Technology, en date du 19 janvier 2005, disponible sur : http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp 105.en.pdf qui reprend le considérant 26 de la directive pour conclure que, dans la plupart des cas, les données créées par les émissions d'un RFID sont des données à caractère personnel. A notre avis, comme déjà affirmé, un tel raisonnement est contestable dans la mesure où la recherche de l'identité de la personne n'est pas nécessaire pour pouvoir agir vis-à-vis d'elle et qu'on peut dès lors difficilement parler à propos de données relatives à un objet de données à caractère personnel. Le droit est en train de se faire dépasser par la technologie. Une autre définition de la donnée à caractère personnel peut sembler nécessaire, fondée cette fois sur la notion de « contactabilité », c'est-à-dire sur le fait que des données permettent ou non de contacter un individu, d'influencer son comportement ou de prendre une décision vis-à-vis de lui. En l'état actuel du droit, ce critère n'est toutefois pas retenu.

par l'application... »[85]. On songe, par exemple, à l'article 5.2 du projet de recommandation actuellement en discussion qui oblige d'apposer une étiquette mentionnant l'usage du RFID, quand bien même n'y aurait-il pas de donnée à caractère personnel traitée, ou à l'article 7.3, b) qui prévoit qu'à tout le moins « le détaillant devrait permettre la désactivation ou l'élimination de l'étiquette ».

34. Des personnes assujetties à la législation

À propos des personnes assujetties à la directive 2002/58/C.E., on peut comprendre de la même manière la volonté des auteurs de la directive d'éviter soigneusement à propos du fournisseur de services de communication, la notion de « responsables du traitement » au sens de la directive générale. On peut en effet imaginer que le fournisseur d'un service de communication enregistre des données relatives à l'utilisation de terminaux pour lesquels le lien avec l'identité de l'utilisateur soit pratiquement impossible. Ainsi, l'activité de tout fournisseur de service de communication accessible au public, c'est-à-dire dont l'activité consiste en l'acheminement des données ou des réseaux ou en l'accès à de tels réseaux, est réglementée sans nécessairement se fonder sur les règles de la directive générale. Ainsi, les hypothèses de légitimité d'un traitement des données acheminées sont très limitées. Cette restriction s'explique par la nature même de leur intervention, qui est dictée par la seule technologie de communication qui s'impose à tout qui utilise des réseaux. Cette situation particulière d'interface explique le rôle que ces fournisseurs peuvent jouer comme « collaborateur » de l'autorité publique dans la recherche d'informations relatives à l'utilisation des réseaux qui pourraient conduire à l'identification de délinquants[86]. Ce rôle, justifie, on le pressent, la mise sur pied de cahiers des charges ou d'agrément applicables à ces acteurs d'une nature particulière. La révision actuellement en cours de la directive 2002/ 22/C.E.[87] concernant le service universel et les droits des utilisateurs relatifs aux infrastructures de communication électronique assigne par ailleurs à ces opérateurs de réseaux et ces fournisseurs d'accès le devoir d'informer

85. Projet de recommandation « RFID sur la vie privée, la protection des données et la sécurité » de la Commission présenté le 21 février 2008 dans le cadre d'une consultation publique sur cette recommandation, p. 17. Ce projet n'est actuellement plus en ligne sur le site de la Commission dès lors que sa consultation publique est close.

86. C'est tout le débat sur le fameux article 15 de la directive à propos du droit des États de demander la conservation des données de trafic. Le débat a abouti à la directive 2006/24/E.C. du 16 mars 2006 relative à la rétention des données de trafic traitées en relation avec la délivrance de services de communications électroniques et amendant la directive 2002/58, directive adoptée en mars 2006.

87. Sur ce point l'avis rendu le 9 janvier 2009 par le contrôleur européen de protection des données (disponible sur le site : http://www.edps.europa. eu) qui souhaite un élargissement de cette obligation à tout service de la société de l'information comme les fournisseurs de services de santé en ligne, des services bancaires en ligne, etc.

l'autorité de régulation du secteur des communications électroniques, voire les utilisateurs du réseau, de tout incident en matière de sécurité des données à caractère personnel, ainsi en cas d'interception illégale de données ou d'accès illégal à des données stockées par ces opérateurs.

35. Des équipements terminaux

D'autres dispositions de la directive témoignent bien plus encore de cette approche nouvelle. L'article 5.3 traite de l'utilisation des réseaux de communication en vue de stocker des informations ou d'accéder à des informations stockées dans l'équipement terminal d'un abonné ou d'un utilisateur. L'article 14 évoque lui les caractéristiques techniques et la normalisation des équipements terminaux pour préciser au point 3 que, nonobstant le principe du libre marché, des normes peuvent être imposées à la construction de ces équipements afin de les rendre comparatifs avec le droit des utilisateurs de protéger et contrôler l'utilisation de leurs données à caractère personnel. Le rapprochement de ces deux dispositions se justifie par le fait qu'elles concernent toutes deux les équipements terminaux et qu'elles constituent des dispositions clairement en dehors du domaine d'application de la directive, domaine fixé comme il a été rappelé par l'article 3.1. de la directive commentée. Elles ne concernent en effet pas des traitements de données opérées dans le cadre de la fourniture de services de communications électroniques. Leur présence est donc d'autant plus significative.

La première disposition entend prévenir toute intrusion dans l'équipement terminal. On songe aux *cookies*, aux *spywares* mais également à des applications plus légitimes permettant par exemple la mise à jour à distance de programmes téléchargés sur l'ordinateur. L'article vise à donner à l'intéressé une maîtrise plus complète de son équipement, en obligeant le responsable de cette intrusion (le responsable du traitement des données)[88] à donner certaines informations à l'utilisateur du terminal sur la finalité de l'intrusion et à lui permettre de refuser cette dernière. L'idée centrale de telles dispositions est donc d'assurer à l'utilisateur d'un terminal une protection contre toute intrusion de ce qui apparaît comme son domicile virtuel. Sans doute y verra-t-on un retour au principe de l'article 8 de la Convention du Conseil de l'Europe qui entend préserver un espace privé virtuel cette fois et non plus physique où la personne est à l'abri du regard d'autrui ?

88. La mention de données à caractère personnel n'est pas utilisée. On note ici aussi que la question est abordée sans qu'on s'interroge sur l'existence on non d'un traitement de données à caractère personnel. C'est l'équipement terminal qui en tant que tel est visé et qui fait l'objet de la protection réglementaire. On sait que la question de savoir si les *cookies* sont des données à caractère personnel est loin d'être tranchée. Cette disposition rend ce débat inutile.

La récente décision du Tribunal constitutionnel allemand du 27 février 2008 [89] crée sur la base du droit général à la personnalité un tout nouveau droit fondamental à la protection de « la confidentialité et l'intégrité des systèmes d'information technologiques » [90]. Ce nouveau droit fondamental en matière de technologie de l'information doit compléter les droits fondamentaux existants là où ils font défaut et ce, eu égard à l'évolution des technologies et des risques nouveaux liés à cette évolution [91]. On note qu'*in casu* il s'agissait de vérifier la constitutionnalité d'une législation d'un Länder autorisant les autorités policières à s'introduire à distance dans un équipement terminal de manière à établir les traces d'infraction de son utilisateur. Le tribunal condamne de telles pratiques sauf lorsqu'il s'agit de criminalité particulièrement grave et que la mesure fait l'objet d'une ordonnance d'un magistrat.

L'article 14 [92] de la directive 2002/58/C.E. prolonge cette première disposition relative au terminal. Dans la mesure où ce sont les spécifications techniques de fonctionnement du terminal qui permettent ces intrusions ou

89. Sur cette décision déjà citée note 34, lire P. DE HERT, K. de VRIES et S. GUTWIRTH, « La limitation des « fouilles en ligne » par un renouvellement des droits fondamentaux, note au sujet de l'arrêt du Bundesverfassungsgericht du 27 février 2008 (Online Durchsuchung) », à paraître *in R.T.D.I.*, 2009/34, http://www.strada.be. Le Tribunal allemand note que cette protection va plus loin que la protection du lieu physique qu'est la maison ou le domicile dans la mesure où elle s'applique peu importe l'endroit où se situe le portable.

90. « Le paragraphe 5, alinéa 2, numéro 11, phrase 1, alternative 2 qui réglemente l'accès clandestin à un système de technologies de l'information viole le droit général de la personnalité (art. 2, al. 1 en relation avec l'art. 1, al. 1 GG) dans son expression spécifique de droit fondamental à la garantie de la confidentialité et de l'intégrité de systèmes de technologies de l'information. » (attendu 166) (Traduction R. Queck).

91. « Les garanties constitutionnelles des articles 10 et 13 GG ainsi que les formes d'expression du droit général de la personnalité qui ont jusqu'à présent été développées dans la jurisprudence de la Cour constitutionnelle fédérale, ne tiennent pas suffisamment compte du besoin de protection résultant du développement des technologies de l'information » (attendu 181) (Traduction R.Queck). « Le droit à l'autodétermination informationnelle ne tient cependant pas intégralement compte des risques pour la personnalité qui résultent du fait que le particulier dépend pour le développement de sa personnalité de l'utilisation de systèmes de technologies de l'information et qu'à cette occasion il confie des données personnelles au système ou les fournit inévitablement rien que par son utilisation. Un tiers qui accède à un tel système peut se procurer un stock de données potentiellement extrêmement grand et significatif sans avoir besoin d'autres actions de collecte de données et de traitement de données. Dans son importance pour la personnalité de l'intéressé, un pareil accès dépasse de loin des collectes de données singulières contre lesquelles protège le droit à l'autodétermination informationnelle. [...] » (Attendu 200) (Traduction R. Queck).

92. Cet article se fonde sur la disposition de la directive 1999/5/C.E. (du Parlement européen et du Conseil du 9 mars 1999, concernant les équipements hertziens et les équipements terminaux de télécommunications et la reconnaissance mutuelle de leur conformité, *J.O.C.E.*, n° L. 091 du 7 avril,1999 pp. 10-28 EUR-*Lex*, http://eur-lex.europa.eu) qui parmi les *essential requirements* qui doivent être respectés par les producteurs ou distributeurs d'équipements terminaux prévoient outre les questions de sécurité des utilisateurs ou des prestataires du réseau, la protection de la vie privée des utilisateurs.

de manière plus générale certaines atteintes à la protection des données, la Commission se réserve le droit d'imposer aux fabricants d'équipements certaines normes qui assurent la compatibilité du terminal avec le respect des exigences de protection des données. Le document de travail du Groupe dit de l'article 29 sur les enjeux de la protection des données relatifs à la technologie RFID préconise d'ailleurs une réglementation des terminaux RFID en suggérant l'obligation pour les fournisseurs de ces équipements de permettre la désactivation du terminal par l'utilisateur et de prévoir des systèmes de cryptage des messages émis ou à destination de ces terminaux [93].

36. Les traits de ce nouveau régime de protection à venir

Notre propos est de montrer l'attention que la directive 2002/58/C.E. donne, au-delà des questions traditionnelles de protection des données à caractère personnel, au fait technologique que représente le fonctionnement des réseaux, et ce indépendamment des rapports entre la personne concernée et les responsables de traitement, chacun situé aux extrémités du réseau.

Ainsi, la directive permet l'extension de la protection à des catégories de données qui ne sont point nécessairement qualifiables de données à caractère personnel dans la mesure où elles sont liées à des terminaux et non à des personnes.

La directive 2002/58/C.E. dite « vie privée et communications électroniques » pointe le rôle particulier de deux acteurs, indépendamment de leur qualité de responsables de traitement :

- Les opérateurs de réseaux (en ce compris les fournisseurs d'accès à Internet), c'est-à-dire ceux qui fournissent « des systèmes de transmission et le cas échéant, les équipements de communication ou de routage et les autres

À noter que des associations comme CASPIAN aux États Unis proposent également une réglementation des RFID en tant que tels (à cet égard voir le site http://www.spychips.com/press-releases/right-to-know-bill.html *Cf.* également, l'avis « aspects éthiques des implants TIC dans le corps humain » du Groupe européen d'Ethique des Sciences et des Nouvelles Technologies : http://europa.eu.int/comm/european_group_ethics/docs/avis20fr.pdf. La Commission ne semble cependant pas avoir opté pour une réglementation spécifique et a plutôt préparé une recommandation « RFID sur la vie privée, la protection des données et la sécurité » présentée le 21 février 2008 dans le cadre d'une consultation publique sur cette recommandation (N.B. : ce projet n'est actuellement plus en ligne sur le site de la Commission dès lors que sa consultation publique est close). Le projet de recommandation donne des conseils sur la mise en œuvre pratique des principes définis dans la directive 95/46/C.E. sur la protection des données à caractère personnel, dans la directive concernant les équipements hertziens et les équipements terminaux de télécommunications 99/5/C.E. et dans la directive concernant le respect de la vie privée et les communications électroniques 2002/58/C.E. À noter qu'elle distingue, aux articles 4, 5 et 7, les règles applicables selon que l'application RFID traite des données à caractère personnel ou non.

ressources qui permettent l'acheminement de signaux [94] » qui constituent des interfaces obligées entre l'utilisateur du réseau en tant que personne concernée et les multiples acteurs de l'Internet qui pourront traiter les données multiples générées consciemment ou non par l'utilisation du réseau. C'est à eux qu'incombent certains devoirs, tels celui de prévenir des risques liés à l'utilisation du réseau, de garantir la sécurité de ses services, de permettre des restrictions à l'identification de la ligne appelante, etc.

- Les fournisseurs d'équipements terminaux, en particulier - mais non uniquement -, des logiciels de navigation, dont les caractéristiques techniques doivent mettre en œuvre les garanties nécessaires au respect des dispositions de la directive. En particulier, la Directive prévoit la possibilité d'imposer certaines « mesures afin de garantir que les équipements terminaux seront construits de manière compatible avec le droit des utilisateurs de protéger et de contrôler l'utilisation de leurs données à caractère personnel ».

Cette extension est justifiée, selon l'avis du Groupe de l'article 29 rendu en matière de RFID [95], par le considérant 2 de la Directive de 1995 suivant lequel : « les systèmes de traitement de données doivent être au service de l'homme : ... ils doivent respecter leurs droits et libertés fondamentaux, en particulier le droit à la vie privée et contribuer au progrès économique et social, au développement du commerce et au bien être des individus ». Cet appel à la réglementation de la technologie doit se concevoir comme un complément des deux premières approches. Comme il a été montré, la deuxième approche signifiait déjà une rupture avec la première dans la mesure où la notion de vie privée, préoccupation à l'origine des lois de protection des données, s'est effacée au profit d'un régime général de protection des données à caractère personnel et par l'octroi de droits subjectifs aux personnes concernées et d'obligations précises pour les responsables de traitement. La troisième approche ne remet pas en cause ces deux premières approches. Au contraire, elle s'y enracine mais la prise en compte des risques nouveaux liés aux réseaux de communication électronique conduit à un nouvel élargissement de la protection des libertés des citoyens et à la prise en considération de la nécessité d'une réglementation de la technologie des terminaux et de l'infrastructure.

94. Directive 2002/21/C.E., article 1(d).
95. Opinion déjà citée.

B. De l'intérêt des concepts essentiels de nos législations de protection des données

37. De trois mises en garde préalables

Les caractéristiques des technologies nouvelles et des applications qu'elles suscitent et les tendances qui entourent leur mise en œuvre nous amènent à renouveler notre manière d'aborder les questions de vie privée. Au risque de choquer les juristes, auxquels trop souvent la tâche de protéger les données est confiée de manière exclusive, trois mises en garde apparaissent nécessaires.

La première est précisément de quitter nos réflexes juridiques. Ne soyons pas d'abord des juristes. Face aux développements que permettent les applications nouvelles, soyons attentifs à leur dimension sociétaire et à la transformation de nos relations humaines induites par ces applications.

La deuxième est de ne pas croire que le droit est la seule solution aux risques générés par ces applications nouvelles : « Si la technologie constitue le problème, elle en constitue également la solution ». Le droit doit s'appuyer sur la technologie, y renvoyer voire y puiser ses solutions.

La troisième est le rappel des deux mots clés des législations de protection des données : « proportionnalité et transparence ». Il importe de donner à ces concepts leur pleine signification dans le contexte actuel.

Chacun de ces conseils appelle les commentaires suivants.

1. *« Vive le Droit de la protection des données » a ses limites*

38. De quelques exemples

Ne soyons pas exclusivement des juristes techniciens mais élargissons nos considérations à la manière dont les applications des technologies de l'information modifient notre façon de vivre ensemble. Ce n'est que dans cette attention aux usages et aux transformations souvent positives mais parfois sur certains points négatifs que nous pourrons proposer la solution juridique appropriée en complément ou non à des solutions faisant appel à d'autres modes de régulation.

Trois exemples donnés à titre purement illustratifs en témoignent. Le premier concerne les changements induits par les applications dites de gouvernement électronique. On le sait, le développement au sein des administrations de l'utilisation des technologies de l'information et de la communication multiplie les communications entre administrations. Il s'agit tantôt de vérifier auprès d'une autre administration les qualités d'un citoyen, tantôt de contrôler le respect par ce dernier des réglementations, tantôt *a*

priori de déterminer automatiquement les bénéficiaires d'un droit à un bénéfice administratif. Ces transmissions dont on loue l'intérêt tant pour l'efficacité de l'administration que pour la facilité et le respect des droits des citoyens induisent une transformation radicale des relations entre le citoyen et l'Administration désormais en réseaux et non plus constituée de « sites » isolés.

Le citoyen qui introduit une demande de permis de bâtir se trouve face à une administration sans visage qui collecte auprès de multiples sources l'information requise, calcule automatiquement la décision à prendre et rend son verdict. Le citoyen n'est plus identifié face à l'administration que par l'identité électronique et un code secret et au sein de celle-ci par un numéro dit d'identification nationale. Dans le domaine de l'aide sociale, l'analyse des dossiers est réduite à la vérification de quelques caractéristiques fixées *a priori* sans plus aucune prise en considération de la personne, de ses difficultés et de sa situation originale. Bref, le citoyen s'est désincarné, réduit à un « numéro », face à une administration *big brother.*

Le deuxième exemple conduit à s'interroger sur la multiplication, applications réseautiques aidant, des « mutuelles » sectorielles de risques. Ainsi, le secteur des assurances, pour combattre les risques que constituent les fraudeurs, les mauvais payeurs ou les personnes à incidents fréquents, a créé des bases de données communes à la profession. Le danger de la constitution de telles mutuelles réside dans la crainte d'exclusion de certains, désignés par ces listes noires, du bénéfice d'un service pourtant essentiel dans nos sociétés. Ainsi, que deviendra celui qui, fustigé par cette liste, souhaitait conclure un contrat d'assurance automobile nécessaire à sa profession ?

Un dernier exemple nous vient d'un fait divers relaté récemment dans les journaux locaux : une école avait mis au point un système permettant de reconnaître automatiquement les étudiants inscrits grâce à une puce RFID placée dans le cartable de ceux-ci. Un tel placement soulève quelques interrogations juridiques, certes, mais également d'autres tout aussi essentielles et sans doute indispensables si le droit veut accomplir son devoir de pesée des intérêts mis en cause et/ou poursuivis par un traitement. Ainsi, peut-on imaginer le ressentiment de l'enfant entre 5 et 10 ans, vis-à-vis duquel les portes de l'établissement scolaire se ferment tout simplement parce que, la veille, sa maman lui a acheté une nouvelle mallette ! Que dire du surveillant qui constate que sa productivité calculée en fonction du nombre d'enfants présents à la garderie est automatiquement contrôlée par ce système !

39. D'une démarche de « *Technology Assessment* »

Ces trois exemples témoignent de l'intérêt d'une approche *Technology Assessment* qui, au-delà d'une application isolée, met en évidence les conséquences sociétaires d'une innovation. Cette analyse permet par ailleurs de mieux mesurer le risque et l'enjeu de l'application dont l'examen est réclamé de l'autorité en charge de la protection des données. C'est à l'aune de ces réflexions qu'il pourra en effet réellement apprécier la légitimité de l'innovation et l'impact de celle-ci sur nos libertés.

2. *Si la technologie constitue le risque, elle en offre également souvent la solution*

40. Le cas des RFID

Le débat européen récent sur les RFID a amené des conclusions sur la responsabilité des constructeurs d'équipements terminaux et des fournisseurs des systèmes RFID, c'est-à-dire des infrastructures qui englobent tant les systèmes de collecte, de transmission, des données générées par les terminaux RFID que les bases de données dans lesquelles ces données seront analysées et grâces auxquelles les décisions *ad hoc* seront prises. Cet élargissement de la protection des données à une réglementation des infrastructures et des terminaux est indispensable. Comment assurer la protection des données de manière effective, si des solutions techniques ne prennent pas en compte ces exigences et les traduisent efficacement ? Ainsi, pour reprendre l'exemple des RFID, souhaite-t-on, avec le Groupe de l'article 29 [96], permettre que le porteur de la puce puisse aisément désactiver la puce, que le système de transmission utilise les solutions de la cryptographie. Cette approche dite *privacy by design* [97] se fonde sur une réflexion fondamentale traduite pour la première fois par les rédacteurs de la loi française de 1978, « l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale.

Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». À

96. *Working paper on the questions of data protection posed by RFID Technology*, 19 janvier 2005, WP n° 105 disponible sur le site de la Commission européenne : http://www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf.

97. Comme affirmé par A. CAVIOUKAN, Commissioner of Data Protection for the Province of Ontario, Canada, dans l'introduction aux Privacy Guidelines for RFID Information Systems, disponible sur le site : http://www.ipc.on.ca. : « Privacy and Security must be built in from the Outset – at the design Stage ».

partir de ce texte, les organes de protection des données ont à plusieurs reprises affirmé le principe de la responsabilité des fournisseurs d'équipements terminaux et des concepteurs d'infrastructures quant aux risques que l'utilisation de leurs infrastructures ou terminaux pouvaient engendrer vis-à-vis de la protection des données de leurs utilisateurs [98].

La Commission opte pour cette solution dans sa proposition de recommandation « RFID sur la vie privée, la protection des données et la sécurité » [99]. En effet, dans le cadre de la vente au détail, le projet prévoit que, « lorsqu'une application RFID traite des données à caractère personnel ou lorsque l'évaluation d'impact sur la vie privée… fait apparaître une forte probabilité que des données à caractère personnel soient produites en raison de l'utilisation de l'application, le détaillant doit… désactiver l'étiquette RFID au point de vente, à moins que le consommateur ne choisisse de la garder en état de marche ». Dans le cas contraire, l'article 7.3, b) prévoit qu'à tout le moins « le détaillant devrait permettre la désactivation ou l'élimination de l'étiquette ». L'article 7.4 prévoit enfin que « la désactivation ou l'élimination des étiquettes ne doit impliquer aucune réduction ni la cessation des obligations légales du détaillant ou du fabricant envers le consommateur » [100].

41. Au-delà du droit, la technologie au secours du droit

Un second exemple de l'apport de la technologie à la solution des risques qu'encourent nos libertés est la généralisation réclamée des systèmes d'*Identity*

98. Cette responsabilité se déduit du considérant 2 de la directive 95/46 : « les systèmes de traitement sont au service de l'homme… doivent respecter les libertés et droits fondamentaux des personnes, notamment la vie privée… doivent contribuer au progrès économique et social et au bien-être des individus ». Cette responsabilité des fabricants des produits technologiques et des concepteurs des applications de la technologie a été soulignée à plusieurs reprises par le Groupe dit de l'article 29. (Sur ce raisonnement, lire en particulier, Document de travail sur les questions de protection des données posées par la technologie RFID, document du 19 janvier 2005 WP n° 105, disponible sur le site de la Commission : http://www.ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_fr.pdf ; *cf.* également le rapport hollandais de R. BEUGELSDIJK publiée par la Registratiekamer : « *RFID : Veelbelovend of onverantwoord ?* »,disponible sur le site : http://www.c bpweb.nl

99. Projet de recommandation « RFID sur la vie privée, la protection des données et la sécurité » de la Commission présenté le 21 février 2008 dans le cadre d'une consultation publique sur cette recommandation. Ce projet n'est actuellement plus en ligne sur le site de la Commission dès lors que sa consultation publique est close.

100. Contrairement à la directive 2002/58 du 12 juillet 2002 concernant le traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications électroniques (*J.O.C.E.*, L201/37, 31 juillet 2002, EUR-*Lex*, http://eur-lex.europa.eu) et à son article 5.3, le projet de recommandation prévoit donc que l'on ne devrait pas sanctionner le consommateur soucieux de sa vie privée.

Management qui permettent *a priori* et *a posteriori* de contrôler les demandes d'accès et de communication des données et garantissent ainsi le respect automatique des prescrits en matière de limitations d'usage des données à caractère personnel.

On pourrait multiplier les exemples : ainsi, en matière de *cookies*, les applications permettant le signalement de leur arrivée, leur blocage, la possibilité de refus d'envoi de ceux-ci comme l'exige l'article 5.3 de la directive 2002/58 [101], en matière du non référencement des sites par des sigles *no-robot* automatiquement lisibles par les moteurs de recherche ; c'est l'appel aux *Privacy Enhancing Technologies* [102], aux systèmes de labellisation et au-delà à la collaboration avec les organisations privées ou publiques de standardisation [103].

En conclusion, le droit ne doit pas prétendre tout résoudre. En matière de protection des données, il s'appuiera volontiers sur d'autres modes de régulation parmi lesquelles la régulation par la technologie elle-même tiendra une place considérable [104].

101. Ce que semblent enfin avoir commencé à comprendre les grands concepteurs de navigateur en prévoyant un mode de navigation privée (dans Safari, Chrome, Internet Explorer 8 et Firefox (mais étonnamment par l'adjonction du module complémentaire Distrust)).

102. À ce propos, la communication de la Commission au Parlement européen et au Conseil, *Promouvoir la protection des données par les technologies renforçant la protection de la vie privée*, COM (2007) 228 final, Bruxelles le 2 mai 2007.

103. Sur cette alliance du droit, d'une part, de la technologie et des solutions nées de l'autorégulation, nos réflexions*in* « Droit et technologie – Alliance ou défi », *in Liber Amicorum G. Horsmans*, pp. 943-947.

104. De manière très concrète, la technique fournit donc des parades aux risques d'atteinte à la vie privée. Dans une communication du 2 mai 2007 intitulée « Promouvoir la protection des données par les technologies renforçant la protection de la vie privée » (*cf.* la recommandation citée note 102) la Commission européenne encourage explicitement le développement des technologies renforçant la protection de la vie privée (*privacy enhancing technologies* ou PETs), consciente du fait que « les PET peuvent contribuer au respect par les systèmes d'information et de communication des lois adéquates concernant la protection des données, tout en rendant la violation de ces lois techniquement plus difficile ». Parmi ces technologies renforçant la protection de la vie privée émergent des protocoles permettant l'encryptage ou l'usage de mot de passe afin de protéger les communications entre les lecteurs et les radio-tags, ou encore la mise au point de *blocker tags* qui, placés sur un radio-tag ou à sa proximité, peuvent l'empêcher de communiquer avec un lecteur. Le *kill switch (Kill command* de la norme EPC Gen 2) est un autre dispositif qui permet au consommateur d'exercer son libre choix de désactiver (via passage sous un portique spécial) ou non, et de façon permanente, les radio-tags associés aux produits qu'il a achetés. Il est permis de se demander si les solutions *blocker tags* ou *kill switch* sont intéressantes vu leur mise en œuvre pratique fort contraignante pour le consommateur.

Comme le notent les conclusions du rapport MIAUCE [105], « Le temps est venu pour le droit aussi de demander l'aide de la technologie afin de s'assurer que les mêmes instruments pour l'observation des personnes et des événements (à des fins allant de la sûreté ou de la sécurité à la commercialisation et au divertissement ; par le biais de technologies de l'observation et/ou d'interaction et/ou de profilage) ne refusent pas aux individus de façon disproportionnée et illégitime une protection adéquate de leurs droits fondamentaux et libertés » (traduction libre).

3. *Deux mots clés à prendre au sérieux : transparence et proportionnalité*

42. De la proportionnalité des traitements et de leur contenu

S'il ne fallait retenir que deux concepts de la législation de la vie privée, c'est bien ceux-là [106]. L'examen de leur signification se révèle chaque jour plus délicat vu les implications des applications nouvelles, leur complexité et de manière générale les caractéristiques des technologies nouvelles.

La proportionnalité tout d'abord. Elle s'entend tant de l'existence même du traitement que du contenu de celui-ci. À propos de l'existence du traitement, on se posera les questions suivantes.

N'y avait-il pas d'autres moyens moins attentatoires à la liberté de réaliser le même objectif que celui poursuivi par le traitement ? Ainsi, la recherche d'infractions s'opère certes plus facilement par une utilisation croisée intelligente des traces laissées par les utilisateurs des technologies de communication. Ces traces révèlent la localisation des individus, leurs relations avec autrui, les sites fréquentés, voire les échanges entretenus. Mais, faut-il pour cela exiger la coopération de tous les opérateurs, fournisseurs d'accès ou de services, exiger la conservation par eux de toutes les données de communication et envisager ce mode de preuve pour toute infraction [107] ?

Le profilage des internautes est aisé par le recoupement des données de provenances diverses mais la justification de ce profilage, qu'il soit l'analyse du risque que présente le crédit demandé par un client ou le ciblage publicitaire, justifie-t-il l'atteinte aux libertés que représente ce « réductionnisme » de l'individu ?

43. De quelques considérations critiques sur le consentement, comme fondement de la légitimité des traitements

Enfin, le consentement, lui-même si souvent invoqué par les responsables de traitement comme justification de leurs traitements, doit être analysé à l'aune de ce principe. Sur Internet, le consentement est non seulement trop facilement argué grâce à l'interactivité des réseaux parfois en contrepartie d'avantages dérisoires mais au-delà il est parfois difficile de le refuser là ou le refus laisse suspecter une « anomalie » et rend la personne concernée encline à le donner.

Cette approche est soutenue par l'argument selon lequel le « droit à la protection des données » serait le droit pour l'individu de décider de la diffusion de ses données. Or la personne concernée étant finalement la personne la mieux placée pour décider de cette diffusion, le consentement individuel serait donc nécessairement un fondement légitime pour le traitement de données à caractère personnel. L'argument selon lequel les données à caractère personnel constitueraient la propriété aliénable de la personne concernée ou une marchandise lui appartenant est discutable [108].

En effet, nous pourrions très bien envisager que les données médicales, par exemple, appartiennent autant au patient qu'au médecin en charge de ce

05. *Cf.* la présentation du projet MIAUCE en note 1.

06. Sur la prééminence de ces deux principes, P. DE HERT et S. GUTWIRTH (« Privacy, Data Protection and law enforcement. Opacity of the individuals and Transparency of the power », dans *Privacy and the Criminal Law*, E.CLAES *et alii* (ed.), Interscientia, Antwerpen-Oxford, 2006, p. 74) : « un individu n'a jamais un contrôle absolu sur un aspect de sa vie privée. Bien que les individus aient la possibilité d'organiser leur vie comme il leur plaît, il est évident que cela cause des frictions sociales ou intersubjectives. À ce stade, les droits, les libertés et les intérêts des autres entrent en jeu. Les zones de frictions et de tensions et les conflits créent le besoin d'une mise en balance des droits et des intérêts qui donnent à la vie privée son sens et sa pertinence. Ceci montre clairement que la vie privée est une notion relationnelle, contextuelle et *per se* sociale qui nécessite une substance uniquement quand elle entre en conflit avec d'autres intérêts privés ou publics bien qu'elle soit essentielle pour un État démocratique en raison de sa référence à la liberté. » (traduction libre).

107. Comme dans la directive 2006/24/C.E. du 15 mars 2006 sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communication électronique accessibles au public ou de réseaux publics de communication, *J.O.U.E.*, L105/54, 13 avril 2006, EUR-*Lex*, http://eur-lex.europa.eu.

108. Internet crée de nouvelles possibilités pour les utilisateurs d'exprimer leur consentement. Dans la première version de P 3 P (*Platform for Privacy Preferences*), les utilisateurs d'Internet avaient la possibilité de négocier leurs préférences en matière de vie privée contre des avantages financiers. Cette possibilité fut longuement discutée dans la littérature américaine. Voy., P.M. SCHWARTZ, « Beyond Lessig's Code for Internet Privacy : Cyberspace, Filters, Privacy control and Fair Information Practices », *Wisconsin Law Review*, 2000, pp. 749 et s. ; M. ROTENBERG, « What Larry doesn't Get the Truth », *Stanford Techn. L. Rev.*, 2001,1, disponible sur le site : http://www.sth.stanford.edu/STLR/Articles/01_STLR_1.

dernier et qui a « produit » ces données contenues dans le dossier médical [109]. Dans « l'approche propriétaire », les données à caractère personnel sont considérées comme des marchandises de valeur pouvant faire l'objet de négociations et de transactions avec d'autres personnes à travers des licences [110]. L'approche contractuelle, qui est fort proche de l'approche propriétaire, place l'accord des parties au centre du traitement des données. Sans se demander si les données à caractère personnel sont totalement considérées comme une propriété, cette approche permet aux parties de faire des promesses en ce qui concerne les données à caractère personnel et leur traitement [111]. Shoeman [112] ajoute : « considérer le respect de la vie privée comme un droit ou une habilitation à déterminer quelles sont les informations nous concernant qui sont accessibles par autrui entraîne une difficulté : cela implique que l'on s'interroge sur le statut moral de la vie privée. Cela suppose que la vie privée est une chose qui doit être protégée à la discrétion de l'individu à qui l'information est reliée ».

44. Proportionnalité et logiques dominantes

La proportionnalité s'entend ensuite du contenu des traitements, les technologies de l'information et surtout les capacités de stockage et d'analyse des données qui rendent aisées la collecte et la conservation de plus en plus d'informations et le mouvement de données de plus en plus nombreuses. Toutes ces données sont-elles nécessaires, adéquates et pertinentes ? On rend

09. Tel que l'ont fait remarquer Kang et Buchner : « Mais l'économiste, en créant des droits de propriété en matière de données à caractère personnel ne dit rien sur la personne à laquelle la propriété est attribuée, n'est-ce pas ? Supposons qu'un citoyen a fait l'acquisition d'une quantité importante d'herbes de St Jean auprès d'un vendeur vendredi dernier. Lequel des deux possède la propriété de la connaissance de l'achat réalisé par le citoyen ? Et quelles sont exactement les conséquences d'une telle propriété ? » (traduction libre) (J. KANG & B. BUCHNER, « Privacy in Atlantis », 18 *Harv. Journal Law & Techn.*, 2004, p. 9. Cet article est rédigé sous la forme d'une discussion socratique entre les protagonistes de différentes thèses et les représentants de différentes fonctions de la Société afin de progresser vers un consensus sur les principes de base d'une future législation sur le respect de la vie privée). Cette répartition peut être justifiée, en suivant une approche fondée sur le marché, par la plus grande efficacité de sa solution.

10. En ce qui concerne les similarités qui existent entre ce type de contrats et les contrats de licence portant sur des réalisations protégées par la propriété intellectuelle, voy. P. SAMUELSON, « Privacy as Intellectual Property », 52 *Stanford Law Rev.*, 2000, pp. 1125 et s. ; J. LITMAN, « Information Privacy/Information Property », 52 *Stanford Law Rev.*, 2000, p. 1250 ; K. BASHO, « The Licensing of the personal information. Is that a solution to Internet Privacy ? », 88 *California Law Rev.*, 2000, pp. 1507 et s.

11. J. KANG & B. BUCHNER, « Privacy in Atlantis », 18 *Harv. Journal Law & Techn.*, 2004, p. 4.

12. F. SCHOEMAN, « Privacy Philosophical Dimensions of the Literature », *in Philosophical Dimensions of the Privacy*, F.D. SCHOEMAN (ed.), 1984, p. 3.

le responsable du traitement attentif à ne pas conserver les données indûment [113] et à réserver aux seuls utilisateurs autorisés, les seules données auxquelles ils ont droit.

Le souci de réaffirmer ce principe de proportionnalité se justifie au moment où les logiques de l'efficacité, tant sur le plan de la rentabilité que sur le plan de la sécurité, se voient renforcées grâce aux technologies de l'information et de la communication de manière incroyable.

Ainsi, la sécurité publique, mais également privée, des organisations et des citoyens exige toujours davantage de systèmes de contrôle, de surveillance et d'alerte. La rentabilité économique, au sens le plus large, l'efficacité tout court, viennent comme une justification complémentaire où se rejoignent les préoccupations des administrations et des organisations, d'une part, et les intérêts des consommateurs et des citoyens, intérêts soigneusement mis en évidence par les administrations ou organisations, d'autre part.

45. La transparence des traitements et au-delà des systèmes d'information

Le second mot clé est la transparence des traitements. Certes, on connaît les obligations d'information du responsable des droits d'accès, de rectification et d'opposition des personnes concernées, affirmés par les lois de protection des données à caractère personnel [114]. Mais comment ne pas envisager de renforcer de tels droits et de telles obligations pour permettre à nouveau une certaine égalité des armes » et corriger ainsi la dissymétrie informationnelle croissante entre ceux qui traitent les données sur autrui et précisément ces derniers ? Ainsi, ne faut-il pas obliger à une information sur les circuits d'information, un cadastre des flux, suivis par les informations collectées dans des réseaux d'information complexe ?

113. Voy. les trois principaux moteurs de recherche qui ont ramené la durée de conservation des données à caractère personnel des internautes, pour certains de 24 mois à 9 mois (*Google*), 6 mois (*Microsoft*) et 3 mois (*Yahoo* !) sous la pression du Groupe dit de l'article 29 (Letter dated 12 October 2007 from the Chairman of the Article 29 Working Party to Google regarding their commitment to comply with EU data protection laws, http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007-others_fr.htm).

114. Voy. S. LOUVEAUX et C. de TERWANGNE, « Protection des données à caractère personnel : application en Belgique de la directive européenne », *in Actualités du droit des techniques de l'information et de la communication*, Liège, CUP, 2001, vol. 45, pp. 9-34.

46. De la transparence des terminaux : la technologie au service de la transparence

Ne faut-il pas rendre obligatoire la transparence du fonctionnement de nos terminaux ? La façon dont ils opèrent est telle que certains traitements restent invisibles et sans contrôle ou réelle maîtrise par leurs utilisateurs. Par ailleurs, on s'interroge sur la nécessité d'équipements terminaux transparents dans leur fonctionnement permettant à leur usager d'avoir la pleine maîtrise des données envoyées et reçues. Ainsi, l'usager devrait pouvoir connaître de manière conviviale l'étendue exacte du bavardage de son ordinateur, les informations transmises et reçues, leur finalité et leur émetteur ou leur destinataire. À cette fin le journal de bord apparaît comme une technique appropriée et relativement aisée à mettre en œuvre.

Au-delà de ce droit de l'utilisateur d'être informé des flux entrants, on peut s'interroger sur le droit de la personne de soumettre à autorisation le fait pour un tiers de pénétrer son « domicile virtuel ».

Conclusions

47. Technologie et vie privée : la langue d'Esope

Que les technologies de l'information apportent à chacun une occasion de se ibérer, de découvrir des mondes nouveaux, de s'affranchir des contraintes que tissent son lieu et son cadre d'existence, de s'exprimer et d'entrer en communication avec qui il souhaite est évident. Qu'elles apportent à chacun les avantages tant sur le plan économique (achat à distance, économie de léplacements) que sur le plan de la sécurité (système de vidéosurveillance) est ndéniable.

Ces mêmes technologies représentent un risque d'autant plus grand pour os libertés que les avantages de ces technologies mis en avant nous amènent multiplier les risques : non seulement à accepter d'être suivis, à nous voir éduits à un numéro, à subir les messages qui nous arrivent à tout moment sur os boîtes aux lettres, sur nos écrans, voire dans nos corps, mais au-delà à ouer le jeu de la marchandisation de l'information personnelle, en nous xhibant sur le net à travers les réseaux sociaux et autres.

En cela, notamment, un enjeu essentiel du droit à la protection de la vie rivée est la défense de l'humain, de son développement et de sa dignité omme valeurs absolues et le renvoi des logiques absolues de sécurité et 'efficacité économique à leur dimension toute relative.

Alors que le dogme sécuritaire fait de tout individu un suspect par défaut et que la logique économique en fait un être essentiellement rationnel et égoïste, rendre possible la contestation de ces logiques absolues est d'autant plus urgent qu'à force de déployer, à travers notamment les dispositifs technologiques de la société de l'information, des représentations aussi négatives de l'individu, on risque effectivement, de susciter des comportements qui justifieront *in fine* ces logiques sécuritaires et économiques absolues, mais au prix de la plus précieuse de nos aptitudes : la liberté. A condition d'accepter de remettre en cause ces représentations collectives, nous pourrons faire en sorte que les personnes puissent effectivement déployer tout le potentiel non seulement libératoire, mais aussi créatif et politique contenu en germe dans la société de l'information. Ainsi, le droit à la protection de la vie privée n'apparait-il pas seulement comme un droit fondamental parmi d'autres, mais comme une condition nécessaire à l'exercice des autres droits et libertés fondamentaux.

Voilà, l'enjeu. Pour le relever, les autorités de protection des libertés apparaissent bien démunies. Il ne s'agit pas ici des moyens humains et financiers qui sont mis à leur disposition mais plutôt de l'absence d'alliés. L'État traditionnellement désigné comme garant de nos libertés se montre de plus en plus intéressé par les apports que peuvent lui conférer les technologies en termes d'efficacité et de sécurité. La population elle-même s'avère plus fascinée par les bénéfices de ces mêmes technologies que craintive des risques que leur utilisation génère. La cause des libertés apparaît bien lointaine et difficile à défendre quand les préoccupations des citoyens sont plus dictées par des impératifs à court terme.

Comment relever ce défi ? Sans doute, en levant le voile de l'opacité du fonctionnement des réseaux qui nous entourent, une éducation qui permette de comprendre le sens de législations dont le libellé est trop obscur mais qui prend sens lorsqu'on invite les citoyens à s'interroger sur le sort de toutes les données qu'ils confient à la toile, à *Facebook*, quand on révèle aux consommateurs le fonctionnement de la publicité sur l'Internet ou quand les employés découvrent l'utilisation qui peut être faite des traces que leur utilisation d'un G.P.S. d'un portable ou de leur ordinateur révèle à leurs employeurs.

Forger de nouvelles alliances avec ces représentants de libertés, des consommateurs ou des syndicats est une deuxième tâche pour nos autorités de protection des données. Que ces dernières dans leur combat n'oublient surtout pas qu'elles sont et doivent rester indépendantes !